Cyprus

Cyprus has been divided since the Turkish military intervention of 1974, following a coup d'etat directed from Greece. Since then, the southern part of the country has been under the control of the Government of the Republic of Cyprus. The northern part is controlled by a Turkish Cypriot administration that in 1983 proclaimed itself the "Turkish Republic of Northern Cyprus (TRNC)." The U.S. Government recognizes only the Government of the Republic of Cyprus, and does not recognize the "TRNC".

Republic of Cyprus. The Republic of Cyprus is a major regional financial center with a robust financial services industry, both domestic and offshore, which contributes about 6.1 percent of the country's gross domestic product. Like other such centers, it remains vulnerable to international money laundering activities. Fraud and, to some extent, narcotics trafficking are the major sources of illicit proceeds laundered in Cyprus. Casinos, Internet gaming sites, and bearer shares are not permitted in the Government of Cyprus (GOC)-controlled area of Cyprus, although sports betting halls are allowed.

The development of the offshore financial sector in Cyprus has been facilitated by the island's central location, a preferential tax regime, double tax treaties with 33 countries (including the United States, several European Union (EU) nations, and former Soviet Union nations), a labor force particularly well trained in legal and accounting skills, a sophisticated telecommunications infrastructure, and relatively liberal immigration and visa requirements. In July 2002, Cyprus introduced a major amendment to its tax laws resulting in a uniform tax rate of 10 percent for all enterprises in Cyprus, irrespective of the permanent residence of their owners. This tax revision effectively lifted the distinction between local companies and offshore international business companies (IBCs). Both the prohibition from doing business locally and the preferential tax treatment that distinguished IBCs from local companies have been abolished. A grandfather clause that had allowed existing IBCs to maintain their former tax status of 4.25 percent for a transitional period expired at the end of 2005. As of 1 January 2006, the legal distinction between domestic companies and off shore IBCs ceased.

Similar provisions were introduced for offshore International Banking Units (IBUs), branches or subsidiary companies of established foreign banks, which had cumulative assets of $16.3 billion at the end of 2005. As with the IBCs, the distinction between domestic banks and IBUs ceased on January 1, 2006 upon the expiration of a transition period that had allowed preferential (4.25. percent) tax treatment for IBUs established before 2002. IBUs can do business locally, but for the time being may not offer any banking services whatsoever in Cypriot pounds to either residents or non-residents. This restriction may soon be lifted, as evidenced by the Central Bank's November 2005 decision to require IBUs to hold two percent of their deposits in local currency as minimum reserves with the Central Bank. IBUs are required to adhere to the same legal, administrative, and reporting requirements as domestic banks. The GOC is currently revising its policy regarding the licensing of new foreign-owned bank branches or subsidiaries. Details are not yet available, but Cyprus has become much more selective in terms of aiming to attract only banks from jurisdictions with proper supervisory authorities. IBUs must have a physical presence in Cyprus and cannot be shell banks. Once an IBU has registered in Cyprus, it is subject to a yearly on-site inspection by the Central Bank. The GOC-controlled area of Cyprus hosts 12 domestic banks, and 26 IBUs.

Since May 2004, when Cyprus joined the EU, banks licensed by competent authorities in EU countries may establish branches in Cyprus or provide banking services on a cross-border basis without obtaining a license from the Central Bank of Cyprus, under the EU's "single passport" principle. By the end of 2005, three EU banks that had already been operating as IBUs had elected to continue their presence in Cyprus under the "single passport" arrangement.

Over the past nine years, Cyprus has put in place a comprehensive anti-money laundering legal framework that comports with international standards. The GOC continues to revise these laws to meet evolving international standards. In 1996, the GOC passed the Prevention and Suppression of Money Laundering Activities Law. This law criminalizes both drug and non-drug-related money laundering, provides for the confiscation of proceeds from serious crimes, codifies actions that banks and non-bank financial institutions must take (including customer identification), and mandates the establishment of a Financial Intelligence Unit (FIU). The anti-money laundering law authorizes criminal (but not civil) seizure and forfeiture of assets. Subsequent amendments to the 1996 law broadened its scope by eliminating the separate list of predicate offenses (now defined as any criminal offense punishable by a prison term exceeding one year), addressing government corruption, and facilitating the exchange of financial information with other FIUs, as well as the sharing of assets with other governments. A law passed in 1999 criminalizes counterfeiting bank instruments, such as certificates of deposit and notes.

Amendments passed in 2003 and 2004 implement the EU's Second Money Laundering Directive. These amendments authorize the FIU to instruct banks to delay or prevent execution of customers' payment orders; extend due diligence and reporting requirement to auditors, tax advisors, accountants, and, in certain cases, attorneys, real estate agents, and dealers in precious stones and gems; permit administrative fines of up to $6,390; and increase bank due diligence obligations concerning suspicious transactions and customer identification requirements, subject to supervisory exceptions for specified financial institutions in countries with equivalent requirements.

Also in 2003, the GOC enacted new legislation regulating capital and bullion movements and foreign currency transactions. The new law requires all persons entering or leaving Cyprus to declare currency (whether local or foreign) or gold bullion worth approximately $15,500 or more. This sum is subject to revision by the Central Bank. This law replaces exchange control restrictions under the Exchange Control Law, which expired on May 1, 2004.

The supervisory authorities for the financial sector are the Central Bank of Cyprus, the Securities Commission of the Stock Exchange, the Superintendent of Insurance, the Superintendent of Cooperative Banks, the Councils of the Bar Association and the Institute of Certified Public Accountants. The supervisory authorities may impose administrative sanctions if the legal entities or persons they supervise fail to meet their obligations as prescribed in Cyprus's anti-money laundering laws and regulations.

All banks must report to the Central Bank, on a monthly basis, individual cash deposits exceeding approximately $21,200 in local currency or approximately $10,000 in foreign currency. Bank employees currently are required to report all suspicious transactions to the bank's compliance officer, who determines whether to forward the report to the Unit for Combating Money Laundering (MOKAS), the Cypriot FIU, for investigation. Banks retain reports not forwarded to MOKAS, and these are audited by the Central Bank as part of its regular on-site examinations. Banks must file monthly reports with the Central Bank indicating the total number of suspicious activity reports (SARs) submitted to the compliance officer, and the number forwarded by the compliance officer to MOKAS. By law, bank officials may be held personally liable if their institutions launder money. Cypriot law protects reporting individuals with respect to their cooperation with law enforcement. Banks must retain transaction records for five years.

In recent years the Central Bank has introduced many new regulations aimed at strengthening anti-money laundering vigilance in the banking sector. Among other things, banks are required to (1) ascertain the identities of the natural persons who are the "principal/ultimate" beneficial owners of corporate or trust accounts; (2) obtain as quickly as possible identification data on the natural persons who are the "principal/ultimate" beneficial owners when certain events occur, including an unusual or significant transaction or change in account activity; a material change in the business name, officers, directors and trustees, or business activities of commercial account holders; or a material change in the customer relationship, such as establishment of new accounts or services or a change in the authorized signatories; (3) adhere to the October 2001 paper of the Basel Committee on Banking Supervision on "Customer Due Diligence for Banks"; and (4) pay special attention to business relationships and transactions involving persons from jurisdictions identified by the Financial Action Task Force (FATF) as non-cooperative. This list is updated regularly in line with the changes effected to the list of non-cooperative countries and territories by the FATF.

In November 2004, the Central Bank issued a revised money laundering guidance note that places several significant new obligations on banks, including requirements to develop a customer acceptance policy; renew customers' identification data on a regular basis; construct customers' business profiles; install computerized risk management systems in order to verify whether a customer constitutes a "politically exposed person"; provide full details on any customer sending an electronic transfer in excess of $1,000; and implement (by June 5, 2005) adequate management information systems for on-line monitoring of customers' accounts and transactions. Cypriot banks have responded by adopting dedicated electronic risk management systems, which they typically use to target transactions to and from high-risk countries. Cyprus's Exchange Control Law expired on May 1, 2004, ending Central Bank review of foreign investment applications for non-EU residents. Individuals wishing to invest on the island now apply through the Ministry of Finance. The Ministry also supervises collective investment schemes.

The Central Bank also requires compliance officers to file an annual report outlining measures taken to prevent money laundering and to comply with its guidance notes and relevant laws. In addition, the Central Bank is legally empowered to conduct unannounced inspections of bank compliance records. In July 2002, the U.S. Internal Revenue Service (IRS) officially approved Cyprus's "know-your-customer" rules, which form the basic part of Cyprus' anti-money laundering system. As a result of the above approval, banks in Cyprus that may be acquiring United States securities on behalf of their customers are eligible to enter into a "withholding agreement" with the IRS and become qualified intermediaries.

MOKAS, the Cypriot FIU, was established in 1997. MOKAS is responsible for receiving and analyzing SARs and for conducting money laundering or financial fraud investigations. A representative of the Attorney General's Office heads the unit and its 20-member staff includes 14 full-time personnel, three part-time police officers, and three part-time Customs officers. However, MOKAS staffing is not sufficient to allow it to meet all its responsibilities. Plans to hire eight additional full-time employees have consistently been put on hold due to GOC-wide hiring freezes. MOKAS cooperates closely with FinCEN and other U.S. Government agencies in money laundering investigations.

All banks and non-bank financial institutions-insurance companies, the stock exchange, cooperative banks, lawyers, accountants, and other financial intermediaries-must report suspicious transactions to MOKAS. Sustained efforts by the Central Bank and MOKAS to strengthen reporting have resulted in an increase in the number of SARs being filed from 25 in 2000 to 144 in 2005 (through 14 December). During 2005 MOKAS received 190 information requests from foreign FIUs, other foreign authorities, and INTERPOL. Nine of the information requests were related to terrorism, although not specifically involving Cyprus. MOKAS evaluates evidence generated by its member organizations and other sources to determine if an investigation is necessary. It has the power to suspend financial transactions for an unspecified period of time as an administrative measure. MOKAS also has the power to apply for freezing or restraint orders affecting any kind of property, at a very preliminary stage of an investigation. In 2005, for the first time, MOKAS issued several warning notices, based on its own analysis, identifying possible trends in criminal financial activity. These notices have already produced results, including the closure of dormant bank accounts. MOKAS conducts anti-money laundering training for Cypriot police officers, bankers, accountants, and other financial professionals. Training for bankers is conducted in conjunction with the Central Bank of Cyprus Since late 2003, the MOKAS computer network has been connected with that of the central government, thus giving MOKAS direct access to other GOC agencies and ministries.

During 2005, MOKAS opened 373 cases and closed 134. Reportedly, there was an undetermined number of successful prosecutions. During the same period, it issued 16 Information Disclosure Orders (typically involving judiciary proceedings in courts abroad), 12 administrative orders for postponement of transactions, and nine freezing orders, resulting in the freezing of $1,680.000 in bank accounts and 11 pieces of real estate. Additionally, during 2005 MOKAS issued two confiscation orders for a total amount of $42,000 (in one of the cases, the GOC shared the money with another jurisdiction that had been involved). Government actions to seize and forfeit assets have not been politically or publicly controversial, nor have there been retaliatory actions related to money laundering investigations, cooperation with the United States, or seizure of assets. There have been at least ten convictions recorded under the 1996 Anti-Money Laundering law, and a number of other cases are pending.

On November 30, 2001, Cyprus became a party to the UN International Convention for the Suppression of the Financing of Terrorism. The implementing legislation amended the anti-money laundering law to criminalize the financing of terrorism. In November 2004, MOKAS designated two employees to be responsible for terrorist finance issues. MOKAS routinely asks banks to check their records for any transactions by any person or organization designated by foreign FIUs as a terrorist or a terrorist organization. If a person or entity is so designated by the UN 1267 Sanctions Committee or the EU Clearinghouse, the Central Bank automatically issues a "search and freeze" order to all banks, both domestic and IBUs. As of mid-December 2005, no bank had reported holding a matching account. The lawyers' and accountants' associations cooperate closely with the Central Bank. The GOC cooperates with the United States to investigate terrorist financing.

There is no evidence that alternative remittance systems such as hawala or black market exchanges are operating in Cyprus. The GOC believes that its existing legal structure is adequate to address money laundering through such alternative systems. The GOC licenses charitable organizations, which must file with the GOC copies of their organizing documents and annual statements of account. Reportedly, the majority of all charities registered in Cyprus are domestic organizations.

Cyprus is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Cyprus is a member of the Council of Europe's MONEYVAL, and the Offshore Group of Banking Supervisors. MOKAS is a member of the Egmont Group and has signed memoranda of understanding (MOUs) with the FIUs of the United States, Belgium, France, the Czech Republic, Slovenia, Malta, Ireland, Australia, Ukraine, Poland, Canada, Russia, Bulgaria, South Africa, and Israel. Although Cypriot law specifically allows MOKAS to share information with other FIUs without benefit of an MOU, Cyprus is negotiating MOUs with Venezuela, Italy, and Romania. A Mutual Legal Assistance Treaty between Cyprus and the United States entered into force September 18, 2002. In 1997, the GOC entered into a bilateral agreement with Belgium for the exchange of information on money laundering. Cyprus underwent a MONEYVAL mutual evaluation in April 2005, the results of which will be published in a report to be adopted at the MONEYVAL Plenary meeting in January 2006.

The Government of the Republic of Cyprus has put in place a comprehensive anti-money laundering regime. It should continue to take steps to tighten implementation of its laws. In particular, it should ensure that regulation of charitable and nonprofit entities is adequate. Cyprus should enact provisions that allow for civil forfeiture of assets.

Area Administered by Turkish Cypriots. The Turkish Cypriot community continues to lack the legal and institutional framework needed to provide effective protection against the risks of money laundering. Turkish Cypriot authorities have, however, developed a greater appreciation of the dangers of unchecked money laundering and have begun taking limited steps to address these risks. It is believed that the 23 essentially unregulated, and primarily Turkish-mainland owned, casinos are the primary vehicles through which money laundering occurs. Casino licenses are fairly easy to obtain, and background checks done on applicants are minimal. A significant part of the funds generated by these casinos are reportedly transported directly to Turkey without entering the Turkish Cypriot banking system, and there are few safeguards to prevent the large-scale transfer of cash to Turkey. Another area of concern is the 500 "finance institutions" operating in the area administered by Turkish Cypriots that extend credit and give loans. Although they must register with the "Office of the Registrar of Companies" they are unregulated. Some are owned by banks and others by auto dealers. In 2005, there was a huge increase in the number of sport betting halls, which are licensed by the "Ministry of Sports and Youth." There are currently six companies operating in this sector, each of which has between 15 and 20 branches; licenses for two additional companies are pending. The fact that the "TRNC" is recognized only by Turkey limits the ability of Turkish Cypriot officials to receive training or funding from international organizations with experience in combating money laundering.

The offshore banking sector also remains a concern. In August 2004, the U.S. Department of the Treasury's FinCEN issued a notice of proposed rulemaking to impose a special measure against First Merchant Bank OSH Ltd in the area administered by Turkish Cypriots as a financial institution of primary money laundering concern. Pursuant to Section 311 of the USA PATRIOT Act, FinCEN found First Merchant Bank to be of primary money laundering concern based on a number of factors, including: (1) It is licensed as an offshore bank in the "TRNC", a jurisdiction with inadequate anti-money laundering controls, particularly those applicable to its offshore sector; (2) it is involved in the marketing and sale of fraudulent financial products and services; (3) it has been used as a conduit for the laundering of fraudulently obtained funds; and (4) the individuals who own, control, and operate First Merchant Bank have links with organized crime and apparently have used First Merchant Bank to launder criminal proceeds. As a result of the finding and in consultation with federal regulators and the Departments of Justice and State, FinCEN proposed imposition of the special measure that would prohibit the opening or maintaining of correspondent or payable-through accounts by any domestic financial institution or domestic financial agency for, or on behalf of First Merchant Bank OSH Ltd. First Merchant Bank's license has not been revoked or suspended, and it continues to operate.

In 1999, a money laundering law for the area administered by Turkish Cypriots went into effect with the stated aim of reducing the number of cash transactions in the "TRNC" as well as improving the tracking of any transactions above $10,000. Banks are required to report to the "Central Bank" any electronic transfers of funds in excess of $100,000. Such reports must include information identifying the person transferring the money, the source of the money, and its destination. Banks, non-bank financial institutions, and foreign exchange dealers must report all currency transactions over $20,000, and suspicious transactions in any amount. Banks must follow a know-your-customer policy and require customer identification. Banks must also submit suspicious transaction reports to an "Anti-Money Laundering Committee" that is supposed to function as a quasi-FIU and have investigative powers. The five-member committee is composed of representatives of the police, customs, the "Central Bank," and the "Ministry of Finance." However, the 1999 anti-money laundering law has never been fully implemented or enforced.

In 2005, the "Anti-Money Laundering Committee," which had been largely dormant for several years, began meeting on a regular basis and encouraging banks to meet their obligations to file SARs. The committee has reportedly referred several cases of possible money laundering to law enforcement for further investigation, but no cases have been brought to court and no individuals have been charged. There have been no successful prosecutions of individuals on money laundering charges, and there are concerns that law enforcement and judicial officials lack the technical skills needed to investigate and prosecute financial crimes.

Although the 1999 money laundering law prohibits individuals entering or leaving the area administered by Turkish Cypriots from transporting more than $10,000 in currency without prior

"Central Bank" authorization, "Central Bank" officials note that this law is difficult to enforce, given the large volume of travelers to and from Turkey In 2003, Turkish Cypriot authorities relaxed restrictions that limited travel across the UN-patrolled buffer zone. There is also a relatively large British population in the area administered by Turkish Cypriots and a significant number of British tourists. As a result, an informal currency exchange market has developed.

The "Ministries of Finance and Economy and Tourism" are drafting several new anti-money laundering laws that they say will, among other things, better regulate casinos, currency exchange houses, and both onshore and offshore banks. Turkish Cypriot officials have committed to ensuring that the new legislation meets international standards. However, it is unclear if the new legislation will be adopted, and if it is, whether it will ever be fully implemented and enforced.

There are currently 26 domestic banks in the area administered by Turkish Cypriots. Internet banking is available. The offshore sector consists of 18 banks and approximately 50 IBCs. The offshore banks may not conduct business with residents of the area administered by Turkish Cypriots and may not deal in cash. The offshore entities are audited by the "Central Bank" and are required to submit a yearly report on their activities. However, the "Central Bank" has no regulatory authority over the offshore banks and can neither grant nor revoke licenses. Instead, the "Ministry of the Economy" performs this function. Although a proposed new law would have restricted the granting of new bank licenses to only those banks already having licensees in an OECD country, the law never passed.

The 1999 Turkish Cypriot anti-money laundering law does provide better banking regulations than were previously in force, but it is far from adequate. The major weakness continues to be the area administered by Turkish Cypriots many casinos, where a lack of resources and expertise leave that area, for all intents and purposes, unregulated, and therefore especially vulnerable to money laundering abuse. The largely unregulated finance institutions, currency exchange houses, and offshore banking sector are also of concern. The Turkish Cypriot authorities should move quickly to enact a new anti-money laundering law and to tighten regulation of casinos, money exchange houses, and the offshore sector.

Czech Republic

The Czech Republic's central location in Europe and its relatively new status as a functional market economy have left it vulnerable to money laundering. While various forms of organized crime (narcotics trafficking, trafficking in persons, fraud, embezzlement, and smuggling) remain the primary source of laundered assets in the country, Czech officials and media outlets have voiced increasing concern about the ability of extremist groups and terrorists to launder or remit money within the country. Although steadily improving, Czech enforcement and prosecution of money laundering offenses remains relatively weak, with the few convicted offenders receiving only light sentences. Domestic and foreign organized crime groups target Czech financial institutions for laundering activity. Banks, currency exchanges, casinos and other gaming establishments, investment companies, and real estate agencies have all been used to launder criminal proceeds.

The Czech Republic first criminalized money laundering in September 1995 through additions to its Criminal Code. Although the Criminal Code does not explicitly mention money laundering, its provisions apply to financial transactions involving the proceeds of all serious crimes. A July 2002, amendment to the Criminal Code introduces a new, independent offense called "Legalization of Proceeds from Crime." This offense has a wider scope than previous provisions in that it enables prosecution for laundering one's own illegal proceeds (as opposed to those of other parties). The 2002 amendment also stipulated punishments of five to eight years imprisonment for the legalization of proceeds from all serious criminal activity and also called for the forfeiture of assets associated with money laundering.

The Czech anti-money laundering legislation (Act No. 61/1996, Measures Against Legalization of Proceeds from Criminal Activity) became effective in July 1996. A 2000 amendment to the money laundering law requires a wide range of financial institutions to report all suspicious transactions to the Czech Republic's financial intelligence unit (FIU), known as the Financial Analytical Unit (FAU) of the Ministry of Finance. In September 2004, the latest amendments to the money laundering law came into force. The amendments introduce several major changes to the Czech Republic's money laundering laws and harmonize the nation's legislation with the requirements of the Council Directive 2001/97/EC on prevention of the use of the financial system for money laundering (Second 2nd EU Money Laundering Directive). As a result, the list of covered institutions now includes attorneys, casinos, realtors, notaries, accountants, tax auditors, and entrepreneurs engaging in transactions exceeding 15,000 euros.

With regard to terrorist financing, in November 2004, the Czech Government amended the Criminal Code and enacted new definitions for terrorist attacks and for terrorist financing. A penalty of up to 15 years' imprisonment can be imposed on those who support terrorists financially, materially, or by other means. Also, in addition to reporting all suspicious transactions possibly linked to money laundering, covered institutions are now required to report all transactions suspected of being tied to terrorist financing. Multilateral bodies generally agree that the Czech Republic currently possesses an adequate regulatory basis with which to combat money laundering and terrorist financing.

For years, the Czech Republic had been criticized for allowing anonymous passbook accounts to exist within the banking system. Legislation adopted in 2000 prohibits new anonymous passbook accounts. In 2002, the Act on Banks was amended to abolish all existing bearer passbooks by December 31, 2002, and by June 2003 approximately 400 million euros had been converted. While account holders can still withdraw money from the accounts for the next decade, the accounts do not earn interest and cannot accept deposits. In 2003, the Czech National Bank introduced new "know your customer" measures, based on the recommendations of both the Financial Action Task Force (FATF) and the Basel Committee, and created an on-site inspection team. New due diligence provisions became effective in January 2003. The Czech Government is considering placing a limit of 500,000 Czech crowns (approximately $19,250) on the amount of cash that can change hands in cash transactions.

Czech authorities require that financial institutions maintain transaction records for a period of ten years. Reporting requirements also apply to persons or entities seeking to enter the Czech Republic. Under the provisions of the anti-money laundering act, anyone seeking to enter or leave the Czech Republic with more than 350,000 Czech crowns (CZK) (approximately $14,000) in cash, traveler's checks, or other monetary instruments must declare this to customs officials, who are required to forward this information to the FAU of the Ministry of Finance. Similar reporting requirements apply to anyone seeking to mail more than 200,000 CZK (approximately $800) in cash into or out of the country. In practice, however, the effectiveness of these procedures is difficult to assess. With the accession of the Czech Republic to the EU in 2004, nearly all customs stations on the borders were closed. Although the customs station at the Prague Airport remains operational, detecting the smuggling or transport of large sums of currency by highway is difficult.

Since 2000, financial institutions have been required to report all suspicious transactions to the FAU. As the Czech FIU, the FAU has the statutory authority to enforce money laundering and terrorist finance laws. The 2004 amendments to the Anti-Money Laundering Act also extended the anti-money laundering/counterterrorist financing responsibilities of the FAU. The FAU is now authorized to share all information with the Czech Intelligence Service (BIS) and Czech National Security Bureau (NBU). It is hoped that this type of information sharing will improve the timeliness and nature of exchanges between the different agencies within the Czech government. The FAU is also authorized to cooperate and share information with all of its international counterparts, including those not part of the Egmont Group. The FAU also has the ability to freeze assets associated with suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list.

The FAU is an administrative FIU without law enforcement authority and can only investigate accounts for which designated entities have filed suspicious transaction reports. Although the FAU can ask the banking sector to check a specific individual or organization's account, it cannot compel it to do so. It has neither the mandate nor the capacity to initiate or conduct criminal investigations. Investigative responsibilities lie with the Financial Police or other Czech National Police body.

Agency reorganizations in 2003 and 2004 resulted in the establishment of the Unit for Combating Corruption and Financial Criminality (UOKFK), as well as a specialized police unit called the Financial Police (also known as the Illegal Proceeds and Tax Crime Unit). The UOKFK has primary responsibility for all financial crime and corruption cases. The Financial Police are the main law enforcement counterpart to the FAU, and the two agencies work closely together on money laundering cases. In 2004, this partnership resulted in the first formal charges under the revised money laundering statutes.

Although the FAU conducts investigations based on suspicious transaction reports filed by the banks, these examinations only cover a relatively small segment of total financial activity within the Czech Republic. Moreover, the FAU's primary responsibility has been, and remains, identifying cases of tax evasion, which is an endemic problem in the Czech Republic. A May 2001 revision of the Criminal Code facilitates the seizure and forfeiture of bank accounts. A financial institution that reports a suspicious transaction has the authority to freeze the suspect account for up to 24 hours. However, for investigative purposes, this time limit can be extended to 72 hours in order to give the FAU sufficient time to investigate whether or not there is evidence of criminal activity. Currently, the FAU is authorized to freeze accounts for 72 hours. However, the FAU's efforts can be hampered because it often waits for the annual tax submission of suspected individuals before deciding to forward cases to law enforcement for investigation. This often results in the disappearance of funds and property before the police can seize them. If sufficient evidence of criminal activity exists, the case is forwarded to the Financial Police, which have another three days to gather the necessary evidence. If the Financial Police are able to gather enough evidence to start prosecution procedures, then the account can stay frozen for the duration of the investigation and prosecution. If, within the 72 hour time limit, the Financial Police fail to gather sufficient evidence to convince a judge to begin prosecution, the frozen funds must be released. These time limits do not apply to accounts owned by individuals or organizations on the UN 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations.

While the institutional capacity to detect, investigate, and prosecute money laundering and financial offenses has unquestionably increased in recent years, both the FAU and the Financial Police face staffing challenges. Despite recommendations from both the FATF and the Council of Europe's FATF-style regional body (MONEYVAL) regarding the need for FAU staff increases, the government lowered its funding and personnel authorizations in 2005. Although these decisions may be reversed in the future, the FAU remains a relatively small organization, given the scope of its responsibilities. The Financial Police could soon face similar challenges caused by early retirement and the loss of senior investigators. Changes to the police retirement plan and a perceived lack of political support are causing many senior officers to consider early retirement. This could result in potentially devastating effects upon not only the Financial Police, but on organized crime units, anticorruption units, and other critical police organizations as well.

Despite these staffing challenges, an increase in government attention and political will to the problems of money laundering and financial crimes has slightly improved the results of law enforcement and prosecutorial efforts. Prior to 2004, the Czech Republic had not yet had a successful prosecution in a money laundering case. However, in 2004, Ministry of Justice statistics show that prosecutors were able to obtain the first four convictions for attempting to legalize the proceeds from crime. Fifteen people were prosecuted; fourteen were actually accused. One case was suspended and the only penalties imposed were extremely light—only three suspended sentences and a fine. In 2003, there were 36 money laundering cases. There were no resulting convictions in 2003. One ongoing issue is that law enforcement must prove that the assets in question were derived from criminal activity. The accused is not obligated to prove that the property or assets were acquired legitimately.

The number of suspicious transaction reports transmitted to the FAU in 2005 dropped slightly after a significant jump in 2004. The number of inquiries evaluated and forwarded to law enforcement remained unchanged. This trend is interpreted as evidence of the active participation of mandated entities in the anti-money laundering regime. After clarifications to the reporting requirements in 1996, reporting of unusual transactions rose significantly. In 2002, 1,260 suspicious transactions were reported, 1,970 in 2003, 3,267 in 2004, and 2,390 in the period of January through August 2005. The number of reports forwarded to the police remained steady at 115 in 2002 and 114 in 2003. In 2004, the number dropped slightly to 103. From January through August 2005, the figure was again 115 reports. Every case that was passed to law enforcement was investigated.

From January to November 2005, the Department of Criminal Proceeds and Money Laundering investigated 90 cases and seized assets in the value of 900 million CZK (approximately $36 million). This figure is an increase over 2004 when the Department of Criminal Proceeds and Money Laundering investigated 139 cases and seized assets valued at roughly 2 million CZK (approximately $90,000). In 2005, the Department participated in 12 cases investigated by the Czech National Drug Headquarters, and seized assets valued at 48 million CZK (approximately $2 million) and three cars. In comparison, in 2004, the Department participated in 25 cases investigated by the Czech National Drug Headquarters and seized assets valued at 16 million CZK (approximately $700,000).

In October 2005, the Czech Parliament ratified the UN Convention for the Suppression of the Financing of Terrorism. This was a major step, in that it marked both the implementation of the recommendations from international bodies and the completion of the statutory and organizational reforms required to effectively confront this issue. The Czech Government approved the National Action Plan of the Fight Against Terrorism in April 2002. This document covers topics ranging from police work and cooperation to protection of security interests, enhancement of security standards, and customs issues.

In general, Czech authorities have been reliable partners in the battle against terrorist financing. Although the terrorist finance threat in the Czech Republic is generally modest, there is reason to believe that there has recently been an increased possibility of terrorist support activities in the country, and officials have publicly discussed the discovery of small hawala operations remitting funds from the Czech Republic to other parts of the world. The Czech Republic has specific laws criminalizing terrorist financing and legislation permitting rapid implementation of UN and EU financial sanctions, including action against accounts held by suspected terrorists or terrorist organizations. A new government body called the Clearinghouse was instituted in October 2002. It was established under the FAU and functions to streamline the collection of information from institutions in order to enhance cooperation and response to a terrorist threat. The FAU is currently distributing lists of designated terrorists to relevant financial and governmental bodies. Czech authorities have been cooperative in the global effort to identify suspect terrorist accounts. Since September 11, 2001, the FAU has checked the accounts of approximately 1,000 people. An amendment to the anti-money laundering law in 2000 requires financial institutions to freeze assets that belong to suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committees consolidated list. To date, no suspect accounts have been identified in Czech financial institutions, and no terrorist assets have been confiscated.

Asset forfeiture is a relatively new instrument in the hands of Czech prosecutors and investigators. In January 2002, further changes to the Criminal Code were effected which allow a judge, prosecutor, or the police (with the prosecutor's assent) to freeze an account if evidence indicates that the contents were used, or will be used, to commit a crime, or if the contents are proceeds of criminal activity. In urgent cases, the police can freeze the account without the previous consent of the prosecutor, but within 48 hours have to inform the prosecutor, who then confirms the freeze or releases the funds. The Law on the Administration of Asset Forfeiture in Criminal Procedure, passed in August 2003, and effective on January 1, 2004, implements provisions such as handling and care responsibilities for the seizure of property.

The Czech Republic has signed memoranda of understanding (MOUs) on information exchange with Belgium, France, Italy, Croatia, Cyprus, Estonia, Latvia, Lithuania, Poland, Slovenia, Slovakia, and Bulgaria. Formalization of an agreement between the Czech Republic and Europol, the European police office, took place in 2002. The agreement allows an exchange of information about specific crimes and investigating methods, the prevention of crime, and the training of police. Among the most important crimes cited in the cooperation agreement are terrorism, drug dealing, and money laundering.

The FAU is a member of the Egmont Group. The Czech Republic actively participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL); in 2001, it underwent a mutual evaluation by the Committee. The Czech Republic continues to implement changes to its anti-money laundering regime based on the results of the mutual evaluation. In May 2003, the Czech Republic also underwent a financial sector assessment by the World Bank/IMF.

In addition to the UN Convention for the Suppression of the Financing of Terrorism, the Czech Republic is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. The Czech Republic is also a party to the World Customs Organization's Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offenses as well as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

The United States and the Czech Republic have a Mutual Legal Assistance Treaty (MLAT), which entered into force on May 7, 2000, as well as an extradition treaty that has been in effect since 1925. In late 2005, the United States and the Czech Republic completed negotiations on a supplemental extradition treaty and a supplemental MLAT to implement the U.S.-EU Agreements on these subjects. The supplemental agreements are expected to be signed in early 2006.

The Czech Republic has made progress in its efforts to strengthen its money laundering regime, as demonstrated by its ratification of the UN Convention on the Suppression of the Financing of Terrorism and its expanded capacity to enforce existing money laundering regulation despite the threat of future personnel shortages. However, further improvement is still needed. The Czech Republic has to date made only incremental and limited progress in its law enforcement efforts. Prosecutions are still infrequent and penalties have been far too light to serve as an effective deterrent. Standards of proof remain extremely high and gaps in Czech law still allow family members to effectively shield the proceeds of illicit activity. Furthermore, the Czech Republic should enhance its asset forfeiture regime by simplifying the forfeiture of jointly owned assets and allowing for the confiscation of substitute assets. It should ratify the UN Convention against Transnational Organized Crime.

Djibouti

Djibouti is one of the more stable countries in the Horn of Africa. It is a financial hub in the sub-region, thanks to its U.S. dollar-pegged currency and its unrestricted foreign exchange. Officials from the Central Bank have not reported any recent instances of money laundering. Informal and black markets for goods remain important. Smuggled goods consist primarily of highly taxed cigarettes and alcohol. The Djibouti Free Zone (DFZ), managed by Dubai's Jebel Ali Free Zone, was inaugurated in June 2004. Once fully operational, the DFZ will approve and deliver licenses for up to 85 companies.

Djibouti is not considered an offshore financial center but offshore institutions are permitted in the DFZ. Two existing commercial banks handle the bulk of financial transactions. The remainder of the demand is met by a growing number of hawaladars. The Central Bank makes efforts to closely monitor the activities of both the commercial banks and hawaladars. Due to Djibouti's location on the Horn of Africa and its cultural and historical trading ties, Djibouti-based traders and brokers are active in the region. Trade goods often provide counter valuation or a means of balancing the books in hawala transactions.

Djibouti is a party to the 1988 UN Drug Convention. Djibouti signed the United Nations International Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, which entered into force on May 23rd, 2001. Djibouti has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. Legislation criminalizing the financing of terrorism, consistent with UNSCR 1373, is included in the Anti-Money Laundering Law passed in December 2002 as Law No. 196/AN/02/4emeL.

The Anti-Money Laundering Law applies to financial institutions of all forms as well as professionals involved in financial matters. Regulated activities include money deposits, insurance, investment, real estate, casinos and entertainment. The legislation also addresses international cooperation and allows for the freezing or seizing of assets in suspected terrorist finance cases. The government regularly circulates the names of individuals and entities included on the UNSCR 1267 Sanctions Committee's consolidated list. The law also requires financial institutions to verify customer information, including current residence. This verification process promotes rigorous transparency and strict control of transactions. Furthermore, it imposes criteria for: customer identification; communication of information; documentation related to international cooperation; surveillance procedures for suspect accounts; and legal protection of professional secrecy for individuals reporting suspect transactions.

Professionals convicted of facilitating money laundering or terrorist financing can face five to ten years in jail and a fine of DF 25 to 50 million (approximately $141,300 to $282,600). A financial professional who fails to report suspect transactions is liable for fines ranging from DF 10 to 25 million (approximately $56,500 to 141,300). The Department of Treasury receives the proceeds of any assets seized or forfeited in terrorist financing cases.

Djibouti does not have an agreement with the United States government to exchange information on money laundering, but Central Bank officials have repeatedly indicated they would fully cooperate if requested. Djibouti has a formal, bilateral agreement with Ethiopia for the exchange of information and extradition in criminal cases. Furthermore, the anti-money laundering legislation stipulates that Djibouti will cooperate with other countries by exchanging information, assisting in investigations, providing mutual technical assistance and facilitating the extradition process in money laundering cases. In addition, the Central Bank plans to set up a financial intelligence unit (FIU) in early 2006.

The FIU will be housed within the Central Bank and staffed with senior employees who come under the Governor's direct supervision. The purpose of the FIU is to collect information on potential clandestine or criminal financial networks and to become the expert office on identifying money laundering. The FIU may obtain any record or databank upon request from government entities or financial institutions. It will perform analytical duties and assist the Ministry of Interior (Police) and the Ministry of Justice in any financial criminal investigation. The FIU may enter into agreement with foreign FIUs to share information if the foreign FIUs are bound by similar rules of confidentiality and secrecy. Finally, the FIU will provide guidance to the banking community in the fight against counterfeit money, including American dollars.

The Government of Djibouti should accede to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. While Djibouti took a positive step by adopting anti-money laundering legislation, enforcement of the law remains a major challenge. Though Djibouti makes an effort to control all formal transaction points, a large number of hawaladars escape Central Bank regulation. Corruption is also a concern. Corrupt customs officials can easily be tempted to allow large amounts of money or trade goods that transfer value to pass through the borders without any declaration. There is also a history of politically powerful and criminally “untouchable” individuals protecting suspicious financial institutions. Finally, Djibouti must also ensure that an effective anti-money laundering regime is extended to the Djibouti Free Zone as it becomes established.

Dominica

The Commonwealth of Dominica initially sought to attract offshore dollars by offering a wide range of confidential financial services, low fees, and minimal government oversight. A rapid expansion of Dominica’s offshore sector without proper supervision made it attractive to international criminals and vulnerable to official corruption. In response to international criticism, Dominica enacted legislation to address many of the deficiencies in its anti-money laundering regime. Dominica’s financial sector includes one offshore and four domestic banks, 17 credit unions, approximately 9,000 international business companies (IBCs) (a significant increase from 1,435 in 2002), 18 insurance agencies, and one operational Internet gaming company (although reports indicate more Internet gaming sites exist). There are no free trade zones in Dominica. Under Dominica’s economic citizenship program, individuals can purchase Dominican passports and, in the past, official name changes for approximately $75,000 for an individual and $100,000 for a family of up to four persons. Although it was not very active in 2005, Dominica’s economic citizenship program does not appear to be adequately regulated. Individuals from the Middle East, the former Soviet Union, the Peoples’ Republic of China and other foreign countries have become Dominican citizens and entered the United States via a third country without visas. Subjects of United States criminal investigations have been identified as exploiting Dominica’s economic citizenship program in the past.

In June 2000, the Financial Action Task Force (FATF) placed Dominica on its Non-Cooperative Countries and Territories (NCCT) list. As a result, Dominica implemented and revised anti-money laundering reforms and was removed from the NCCT list in October 2002. One of the reforms created was an Offshore Financial Services Council (OFSC). The OFSC’s mandate is to advise the Government of the Commonwealth of Dominica (GCOD) on policy issues relating to the offshore sector and to make recommendations with respect to applications by service providers for licenses. Under common banking legislation enacted by its eight member jurisdictions, the Eastern Caribbean Central Bank (ECCB) acts as the primary supervisor and regulator of onshore banks in Dominica. A December 2000 agreement between the OFSC and the ECCB places Dominica’s offshore banks under the dual supervision of the ECCB and the GCOD Financial Services Unit (FSU). In compliance with the agreement, the ECCB assesses applications for offshore banking licenses, conducts due diligence checks on applicants, and provides a recommendation to the Minister of Finance. The Minister of Finance is required to seek advice from the ECCB before exercising his powers with respect to licensing and enforcement.

The ECCB also conducts on-site inspections for anti-money laundering compliance of onshore and offshore banks in Dominica. Inspections of the offshore banks are conducted by the ECCB in collaboration with the FSU. The ECCB is unable to share examination information directly with foreign regulators or law enforcement personnel; however, legislation to permit such sharing is being drafted. The Offshore Banking (Amendment) Act No. 16 of 2000 prohibits the opening of anonymous accounts, prohibits IBCs from direct or indirect ownership of an offshore bank, and requires disclosure of beneficial owners and prior authorization to changes in beneficial ownership of banks. All offshore banks are required to maintain a physical presence in Dominica and to have available for review on-site books and records of transactions.

The International Business Companies (Amendment) Act No. 13 of 2000 requires that bearer shares be kept with an "approved fiduciary" that is required to maintain a register with the names and addresses of beneficial owners. Additional amendments to the Act in September 2001 require previously issued bearer shares to be registered. The Act empowers the FSU to "perform regulatory, investigatory, and enforcement functions" over IBCs. The FSU staff normally consists of an Acting Manager, two professional staff (supervisors/examiners), and one administrative assistant. The IBU supervises and regulates offshore entities and domestic insurance companies. The IBU also supervises, regulates, and inspects Dominica's registered agents and visits IBCs to ensure that the companies are operating in compliance with requirements imposed by law.

The Money Laundering Prevention Act (MLPA) No. 20 of December 2000 and its July 2001 amendments criminalize the laundering of proceeds from any indictable offense. The MLPA overrides secrecy provisions in other legislation and requires financial institutions to keep records of transactions for at least seven years. The MLPA also requires persons to report cross-border movements of currency that exceed $10,000 to the financial intelligence unit (FIU).

The MLPA establishes the Money Laundering Supervisory Authority (MLSA) and authorizes it to inspect and supervise non-bank financial institutions and regulated businesses for compliance with the MLPA. The MLSA is also responsible for developing anti-money laundering policies, issuing guidance notes, and conducting training. The MLSA consists of five members: a former bank manager, the IBU manager, the Deputy Commissioner of Police, a senior state attorney, and the Deputy Comptroller of Customs. The MLPA requires a wide range of financial institutions and businesses, including any offshore institutions, to report suspicious transactions simultaneously to the MLSA and the FIU. Additionally, financial institutions are required to report any transaction over $5,000.

The May 2001 Money Laundering Prevention Regulations apply to all onshore and offshore financial institutions including banks, trusts, insurance companies, money transmitters, regulated businesses, and securities companies. The regulations specify know your customer requirements, record keeping, and suspicious transaction reporting procedures, and require compliance officers and training programs for financial institutions. The regulations require that the true identity of the beneficial interests in accounts be established, and mandate the verification of the nature of the business and the source of the funds of the account holders and beneficiaries. Anti-Money Laundering Guidance Notes, also issued in May 2001, provide further instructions for complying with the MLPA and provide examples of suspicious transactions to be reported to the MLSA.

The FIU was also established under the MLPA and became operational in August 2001. The FIU's staff consists of a certified financial investigator and a Director. The FIU analyzes suspicious transaction reports (STRs) and cross-border currency transactions, forwards appropriate information to the Director of Public Prosecutions, and carries on liaison with other jurisdictions on financial crimes cases. The FIU has access to the records of financial institutions and other government agencies, with the exception of the Inland Revenue Division. In 2005, the FIU received 19 STRs, which is a significant decrease compared to the 109 STRs received in 2004. The FIU is closely examining the relationship between narcotics proceeds and money laundering in Dominican financial institutions. However, the GCOD believes most of the money laundering cases under investigation involves external proceeds from fraudulent investment schemes.

There are no known convictions on money laundering charges in Dominica. In 2005, a Haitian national was arrested for human trafficking and money laundering. The GCOD also filed criminal complaints against St. Regis University for issuing fraudulent degrees and laundering the proceeds in an offshore bank.

Since 2003, the GCOD has collaborated closely with U.S. and foreign law enforcement agencies in a widespread money laundering case involving European fraudulent investment scheme proceeds in one of the now closed offshore banks in Dominica. As a result of this case, money laundering prosecutions are being brought in the United States, the United Kingdom, and Germany.

On June 5, 2003, Dominica enacted the Suppression of Financing of Terrorism Act (No. 3 of 2003), which provides authority to identify, freeze, and seize terrorist assets, and to revoke the registration of charities providing resources to terrorists. To date, no accounts associated with terrorists or terrorist entities have been found in Dominica. The GCOD has not taken any specific initiatives focused on alternative remittance systems.

In May 2000, a mutual legal assistance treaty between Dominica and the United States entered into force. The GCOD also has a tax information exchange agreement with the United States. The MLPA authorizes the FIU to exchange information with foreign counterparts. The Exchange of Information Act 2002 provides for information exchange between regulators. The MLPA provides for freezing of assets for seven days by the FIU, after which time a suspect must be charged with money laundering or the assets released; assets may be forfeited after a conviction.

Dominica is a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). Dominica is also a member of the Caribbean Financial Action Task Force (CFATF) and underwent its second mutual evaluation in September 2003. Dominica's FIU was accepted into the Egmont Group in June 2003. Dominica is a party to the 1988 UN Drug Convention. Dominica acceded to the UN International Convention for the Suppression of the Financing of Terrorism and to the Inter-American Convention Against Terrorism in September 2004.

The Government of the Commonwealth of Dominica should fully implement and enforce the provisions of its legislation and provide additional resources for regulating offshore entities, including its Internet gaming entities. Dominica should continue to develop the FIU to enable it to fulfill its responsibilities and cooperate with foreign authorities. Dominica should eliminate its program of economic citizenship.

Dominican Republic

The Dominican Republic continues to be a major transit country for drugs. As such, the Dominican Republic's financial institutions engage in currency transactions involving international narcotics trafficking proceeds that include significant amounts of U.S. currency or currency derived from illegal drug sales in the United States. The smuggling of bulk cash by couriers and wire transfer remittances are the primary methods for moving illicit funds from the United States into the Dominican Republic. Once in the Dominican Republic, currency exchange houses, money remittance companies, free trade zones, and casinos facilitate the laundering of these illicit funds.

The 2003 collapse of the country's third largest bank, Banco Intercontinental (Baninter), is a significant example of the corruption and money laundering scandals that continue to plague the financial sector. The Baninter case saw approximately $2.2 billion evaporate over the course of just a few years due to the fraudulent accounting schemes orchestrated by senior officials. The failure of Baninter and two other banks (Banco Mercantil and Bancredito) cost the Government of the Dominican Republic (GODR) in excess of $3 billion and severely destabilized the country's finances. Criminal prosecutions are underway in all three cases. Various legal maneuvers delayed but have not dismissed the criminal prosecution of five Baninter banking officials; an October 2005 decision is currently under appeal. Weaknesses in this sector still have not been fully resolved. The GODR negotiated an IMF standby in August 2003, to help cover the costs of the failures. The IMF insisted on extensive changes in laws and procedures in order to improve banking supervision, which included required passage of law setting procedures for cases of systemic risk to the banking system. These changes have been made and full implementation is expected by mid-2006.

Narcotics-related money laundering was deemed a criminal offense by the enactment of Act 17 of December 1995 (the 1995 Narcotics Law). In 2002, the GODR passed Law No. 72-02 to expand money laundering predicate offenses beyond illegal drug activity and controlled substances, to include other serious crimes, such as any act related to terrorism, illicit trafficking in human beings or human organs, arms trafficking, kidnapping, extortion related to recordings and electronic tapes made by physical or moral entities, theft of vehicles, counterfeiting of currency, fraud against the State, embezzlement, and extortion and bribery related to drug trafficking.

Under Decree No. 288-1996, the Superintendence of Banks decree, banks, currency exchange houses, and stockbrokers are required to know and identify their customers, keep records of transactions (five years), record currency transactions greater than $10,000, and file suspicious transactions reports (STRs). Law No. 72-02 broadens the requirements for customer identification, record keeping of transactions, and reporting of suspicious activity reports (SARs). Numerous other financial sectors are now covered, including securities brokers, the Central Bank, cashers of checks or other types of negotiable instruments, issuers/sellers/cashers of travelers checks or money orders, credit/debit card companies, funds remittance companies, offshore financial service providers, casinos, real estate agents, automobile dealerships, insurance companies, and certain commercial entities such as those dealing in firearms, metals, archeological artifacts, jewelry, boats, and airplanes. The law mandates that these entities are to report currency transactions exceeding $10,000, as well as suspicious transactions. Moreover, the legislation requires individuals to declare cross-border movements of currency that are equal to or greater than the equivalent of $10,000 in domestic or foreign currency.

Two asset seizure laws were recently clarified by an executive order stating that the measures set forth in Law No. 78-03 prevail over those contained in Law No. 72-02. Law No. 78-03 permits the seizure, conservation and administration of assets which are the product or instrument of criminal acts pending judgment and sentencing. The 1995 Narcotics Law allows preventive seizures and criminal forfeiture of drug-related assets, and authorizes international cooperation in forfeiture cases. While numerous narcotics-related investigations were initiated under the 1995 Narcotics Law, and substantial currency and other assets were confiscated, there have been only three successful money laundering prosecutions under this law. In 2005, nine money laundering cases related to narcotics were submitted to the justice system.

Although the GODR and the United States have not put in place a mutual legal assistance treaty, according to U.S. law enforcement officials cooperation between law enforcement agencies on drug cases, human trafficking, and extradition matters remains strong. The GODR continues to support U.S. Government efforts to identify and block terrorist-related funds. Although no assets were identified or frozen, the GODR's efforts to identify and block terrorist-related funds continue through orders and circulars issued by the Ministry of Finance and the Superintendence of Banks that instruct all financial institutions to continually monitor accounts.

The Unidad de Inteligencia Financiera (UIF) was created in 1997 and is located within the Superintendency of Banks. The UIF is an administrative financial intelligence unit that supervises within the financial sector the application of the rules and regulations against money laundering and terrorist financing. Law No. 72-02 created the Unidad de Analisis Financiero (UAF) under the national drug council (CND), to receive STRs from the newly mandated entities and to ensure efficient function of the system of registrations and analysis of information. The powers of UAF supersede those of the UIF. This unit has investigative authority and will also provide support to other competent authorities on any phase of a financial investigation. Law No. 72-02 obligates the UIF to forward all STRs it receives from financial institutions, money exchangers, and remittance companies to the UAF. Since May 2005, the UAF has received 76 STRs and 8505 reports of currency transactions above the legal limit. As of December 2005, the UAF had received only one report from an entity other than the UIF.

The UIF has been a member of the Egmont Group since June 2000; however, it is expected that the UAF will apply for Egmont membership to replace the UIF. The Dominican Republic is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The Dominican Republic is a party to the 1988 UN Drug Convention. The GODR has signed, but has not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The UN Convention Against Corruption was submitted to the Congress for ratification on April 18, 2005, and is expected to be ratified in 2006.

The Government of the Dominican Republic has the legislative framework to combat money laundering and terrorist financing, but insufficient implementation leaves the country vulnerable to criminal financial activity and abuse.

Ecuador

With a dollar economy and a geographical situation between two major drug producing countries, Ecuador is highly vulnerable to money laundering but is not considered an important regional financial center. Because thus far there has been no effective control of money laundering, there is no reliable way to judge the magnitude of such activity in the country. In addition to concerns about illicit transactions through financial institutions, there are some indications that money laundering is taking place through trade and commercial activity. Large amounts of unexplained currency entering and leaving Ecuador indicate that transit and laundering of illicit cash are also significant activities. Though smuggled goods are regularly brought into the country, there is no evidence that they are significantly funded by drug proceeds.

On October 18, 2005, Ecuador’s new comprehensive law against money laundering was published in the country’s Official Register. The new law, Law 2005-13, criminalizes the laundering of illicit funds from any source and penalizes the undeclared entry of more than $10,000 in cash. The law calls for the creation of a financial intelligence unit (FIU) under the purview of the Superintendence of Banks. Regulations for application of the law and establishment of the FIU have not yet been developed.

A free trade zone law was passed in 1991 in order to promote exports, foreign investment, and employment. The law provides for the import of raw materials and machinery free of duty and tax; the export of finished and semi-processed goods free of duty and tax; and tax exemptions for business activities in the government-established zones. Free trade zones have been established in Esmeraldas, Manabi and Pichincha provinces, and a new zone is planned for the site of the new Quito airport. There is no known evidence to indicate that the free trade zones are being used in trade-based money laundering.

Prior to the passage of the 2005 law, the Narcotics and Psychotropic Substance Act of 1990 (Law 108) criminalized money laundering activities only in connection with illicit drug trafficking. Under the new law, money laundering is now criminalized in relation to any illegal activity, including narcotics trafficking, trafficking in persons, and prostitution, among others. Money laundering is penalized by a prison term of three to nine years, depending upon the amount laundered, as well as a monetary fine. All entities that fall under the 1994 Financial System Law, including financial institutions and insurance companies, are required to report all “unusual and unjustified” transactions to the FIU, once it has been established. Obligated entities are also required to maintain registries of cash transactions exceeding $10,000, establish “know-your-client” provisions, and maintain financial transaction records for ten years. Any person entering or leaving Ecuador with $10,000 or more must file a report with the Customs service. Entities or persons who fail to file the required reports or declarations may be sanctioned by the Superintendence of Banks. The FIU may request information from any of the obligated entities to assist in its analysis of suspicious transactions, and cases that are deemed to warrant further investigation will be sent to the Public Ministry. The FIU is also empowered to exchange information with other financial intelligence units on the basis of reciprocity.

There are some weaknesses that were not corrected by the 2005 law. For example, the definition of suspicious transactions as "unusual and unjustified," may allow defendants to use this definition to their advantage in legal proceedings by claiming that the bank did not prove suspicious transactions were "unjustified" and therefore should not have reported the transaction. The wording may also open a loophole for banks and their employees to avoid reporting suspicious transactions by claiming that the transactions were justified to the satisfaction of the bank. Legal protections for financial institutions and their employees who report suspicious transactions are not included in the 2005 law, leaving them vulnerable to legal actions from the subject of the report. Some existing laws may also conflict with the detection and prosecution of money laundering. For example, the Bank Secrecy Law severely limits the information that can be released by a financial institution directly to the police as part of any investigation, and the Banking Procedures Law reserves information on private bank accounts to the Superintendence of Banks. In addition, the Criminal Defamation Law sanctions banks and other financial institutions that provide information about accounts to police or advises the police of suspicious transactions if no criminal activity is proven. As a result of this contradictory legal framework, cooperation between other Government of Ecuador (GOE) agencies and the police has fallen short of the level needed for effective enforcement of money laundering statutes.

Several Ecuadorian banks maintain offshore offices. The Superintendence of Banks is responsible for oversight of both offshore and onshore financial institutions. Regulations are essentially the same for onshore and offshore banks, with the exception that offshore deposits no longer qualify for the government's deposit guarantee. Anonymous directors are not permitted. Licensing requirements are the same for offshore and onshore financial institutions. However, offshore banks are required to contract external auditors pre-qualified by the Superintendence of Banks. These private accounting firms perform the standard audits on offshore banks that would generally be undertaken by the Superintendence in Ecuador. Bearer shares are not permitted for banks or companies in Ecuador.

The 2005 law establishes a National Council Against Money Laundering, to be headed by the director of the FIU and include representatives of all government entities involved in fighting money laundering, such as the Superintendence of Banks and the National Police. The National Council Against Money Laundering will be responsible for administrating the freezing and seizure of funds that are identified as originating from illicit sources. A special fund for forfeited assets will be set up in the Central Bank, and these assets will be distributed among government entities responsible for combating money laundering.

The Ministry of Foreign Affairs, Superintendence of Banks and the Association of Private Banks formed a working group in December 2004 to draft a law against terrorist financing. By year-end 2005, a draft law had been completed and sent to the Presidency for review. Pending promulgation of a new law, terrorist financing has not been criminalized in Ecuador. The Superintendence of Banks has cooperated with the USG in requesting financial institutions to report transactions involving known terrorists, as designated by the United States as Specially Designated Global Terrorists pursuant to Executive Order 13224 (on terrorist financing) or as named on the consolidated list maintained by the UN 1267 Sanctions Committee. No terrorist finance assets have been identified to date in Ecuador. The Superintendence would have to obtain a court order to freeze or seize such assets in the event they were identified in Ecuador. Ecuador has ratified the UN International Convention for the Suppression of the Financing of Terrorism. No steps have been taken to prevent the use of gold and precious metals to launder terrorist assets. Currently, there are no measures in place to prevent the misuse of charitable or non- profitable entities to finance terrorist activities.

Ecuador is a party to the 1988 UN Drug Convention and has ratified the UN Convention against Transnational Organized Crime. In September 2005, Ecuador ratified the UN Convention Against

Corruption, which entered into force December 14, 2005. The GOE has signed, but not yet ratified, the Inter-American Convention Against Terrorism. Ecuador is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Financial Action Task Force of South America Against Money Laundering (GAFISUD). Ecuador and the United States have an Agreement for the Prevention and Control of Narcotic Related Money Laundering that entered into force in 1993 and an Agreement to Implement the United Nations Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances of December 1988, as it relates to the transfer of confiscated property, securities and instrumentalities. There is also a Financial Information Exchange Agreement (FIEA) between the GOE and the U.S. to share information on currency transactions.

During the past five years, there have not been any serious investigations of money laundering in Ecuador. However, the passage of a comprehensive anti-money laundering law represents a major advancement for Ecuador in 2005. The GOE now needs to develop the supporting rules and regulations to enact the legislation in order to effectively govern the collection, analysis, and dissemination of financial intelligence. Ecuador is one of only two countries in South America that is not a member of the Egmont Group of financial intelligence units. Now that the necessary legislative framework exists, the GOE should strive to establish a fully functioning FIU that meets the standards of the Egmont Group and the Financial Action Task Force. The GOE should also correct the deficiencies that were not accounted for in the new money laundering legislation. Ecuador should criminalize the financing of terrorism in order to fully comply with international anti-money laundering and counterterrorist financing standards.

Egypt, The Arab Republic of

Egypt is not considered a regional financial center. In 2005, the Government of Egypt (GOE) continued financial sector reforms that were initiated in 2004, with the aim of streamlining the financial sector. Despite banking sector reform, Egypt is still largely a cash economy, and many financial transactions do not enter the banking system at all.

While there is no significant market for illicit or smuggled goods in Egypt, authorities say that under-invoicing of imports and exports by Egyptian businessmen is a relatively common practice. The primary goal for businessmen who engage in such activity is reportedly the avoidance of taxes and customs fees. It is unclear to what extent price manipulation may be used for laundering the proceeds of other crimes. According to the Ministry of Finance, however, cuts in tariffs in September 2004, followed by cuts in income and business taxes in June 2005, have encouraged businesses to begin following proper procedures and regulations.

At present, money laundering and terrorist financing are not reported to be widespread in Egypt. However, informal remittance systems are unregulated and therefore pose a potential means for laundering funds. Egyptian authorities claim that informal remittances are not widespread in Egypt, but the number of remittances officially recorded by banks does not match the large number of Egyptians working overseas, in the Gulf and elsewhere. Many overseas workers use informal means to remit earnings, due to a lack of trust in or familiarity with banking procedures or to the lower costs associated with informal remittance systems. Due to the unregulated nature of informal remittance systems, it is unclear if and to what extent money laundering actually occurs through these systems. One conventional non-bank money transfer system, Western Union, is starting to draw more customers.

In May 2002, Egypt passed an anti-money laundering law (Law No. 80 of 2002). The law criminalizes the laundering of funds from narcotics trafficking, prostitution and other immoral acts, terrorism, antiquities theft, arms dealing, organized crime, and numerous other activities. The law did not repeal Egypt's existing law on bank secrecy, but it did provide the legal justification for providing account information to responsible civil and criminal authorities. The law also provided for the establishment of the Money Laundering Combating Unit (MLCU) as Egypt's financial intelligence unit (FIU), which officially began operating on March 1, 2003.

In June 2003, the administrative regulations of the anti-money laundering (AML) law were issued as Prime Ministerial Decree No. 951/2003. The regulations provided the legal basis by which the MLCU derives its authority, spelled out the predicate crimes associated with money laundering, established a board of trustees to govern the MLCU, defined the role of supervisory authorities and financial institutions, and allowed for the exchange of information with foreign competent authorities.

Under the anti-money laundering law, banks are also required to keep all records for five years, and numbered or anonymous financial accounts are prohibited. In March 2004, the Central Bank of Egypt (CBE) issued instructions requiring banks to establish internal systems enabling them to comply with the anti-money laundering laws. In addition, banks are now required to submit quarterly reports showing the progress made with respect to their anti-money laundering responsibilities.

The CBE also monitors bureaux de change and money transmission companies for foreign exchange control purposes, giving special attention to those accounts with transactions above certain limits. The Capital Market Authority (CMA), which is responsible for regulating the securities markets, has also undertaken the inspection of firms under its jurisdiction. The inspections were aimed at explaining and discussing anti-money laundering regulations and obligations, as well as evaluating the implementation of systems and procedures, including checking for an internal procedures manual and ensuring the appointment of compliance officers. An independent insurance regulatory authority is planned, and authorizing legislation will likely be submitted to parliament in 2006.

The executive regulations of the anti-money laundering law lowered the threshold for declaring foreign currency at borders from the equivalent of $20,000 to $10,000. The declaration requirement was also extended to travelers leaving as well as entering the country. Enforcement of this provision is not consistent; however, authorities claim that the terrorist attacks of the past year have given extra impetus to law enforcement agencies to thoroughly scrutinize currency imports/exports.

Egypt is not an offshore financial center. Offshore banks, international business companies and other forms of exempt or shell companies are not permitted in Egypt. Egypt has two types of free zones—public and private. Public free zones are specific geographic districts administered by the GOE. Currently, there are ten public free zones in operation. Private free zones are established for a specific project or company to undertake operations such as mixing, repackaging, assembly, and manufacturing for re-export. There is no indication that Egypt's free zones are being used for trade-based money laundering schemes or for financing terrorism.

The MLCU, Egypt's FIU, is an independent entity within the CBE, and has its own budget, staff, and full legal authority to examine all STRs and conduct investigations with the assistance of counterpart law enforcement agencies, including the Ministry of Interior. Presidential Decree No. 164/2002, issued in June 2002, delineates the structure, functions, and procedures of the MLCU. The unit handles implementation of the anti-money laundering law, including publishing the executive directives. The MLCU takes direction from a five-member council, chaired by the Assistant Minister of Justice for Legislative Affairs. Other members include the Chairman of the CMA, the Deputy Governor of the CBE, a representative from the Egyptian Banking Federation, and an expert in financial and banking affairs. In June 2004, the MLCU was admitted to the Egmont Group of FIUs.

The Executive Director of the MLCU is responsible for the operation of the FIU and the implementation of the policies drafted by the Council of Trustees. His responsibilities include: proposing procedures and rules to be observed by different entities involved in combating money laundering; presenting them to the Chairman of the Council of Trustees; reviewing the regulations issued by supervisory authorities for consistency with legal obligations and ensuring that they are up to date; ensuring the capability and readiness of the unit's database; exchanging information with supervisory entities abroad; acting as point of contact within the GOE; preparing periodic and annual reports on the operational status of the unit; and taking necessary action on STRs recommended to be reported to the office of the public prosecution.

Since its inception in 2003, the MLCU has received over a thousand STRs from financial institutions and has successfully brought three cases to court, one involving proceeds from drug smuggling and the other two involving proceeds from antiquities smuggling. All three cases stemmed from domestic rather than foreign criminal activity and all involved individuals rather than criminal networks.

Money laundering investigations are carried out by one of the three law enforcement agencies in Egypt, according to the type of predicate offense involved. The Ministry of Interior, which has general jurisdiction for the investigation of money laundering crimes, has established a separate anti-money laundering (AML) department, which includes a contact person for the MLCU who coordinates with other departments within the ministry. The AML department works closely with the MLCU during investigations. It has established its own database to record all the information it received, including STRs, cases, and treaties. The administrative control authority has specific responsibility for investigating cases involving the public sector or public funds. It also has a close working relationship with the MLCU. The third law enforcement entity, the National Security Agency, plays a more limited role in the investigation of money laundering cases, where the predicate offense threatens national security. The GOE established a national committee for coordinating issues regarding anti-money laundering, which held its first meetings in late 2005.

In 2002, the GOE passed the law on civil associations and establishments (Law No. 84 of 2002), which governs the procedures for establishing non-governmental organizations (NGOs), including their internal regulations, activities, and financial records. The law places restrictions on accepting foreign donations without prior permission from the proper authorities. Both the Ministry of Social Affairs and the CBE continually monitor the operations of domestic NGOs and charities to prevent the funding of domestic and foreign terrorist groups.

Because of its own historical problems with domestic terrorism, the GOE has sought closer international cooperation to counter terrorism and terrorist financing. The GOE has shown a willingness to cooperate with foreign authorities in criminal investigations, whether they are related to terrorism or to narcotics.

In January 2005, the National Committee for Combating Money Laundering and Terrorist Financing was established within the MLCU to coordinate policy implementation among the various responsible agencies of the GOE. The committee includes representatives from the Ministries of Interior, Foreign Affairs, Social Affairs, Justice, and the National Security Agency, in addition to the MCLU. The same agencies sit on a National Committee for International Cooperation in Combating Terrorism, which was established in 1998.

The GOE is in the process of replacing its original counterterrorism law, an emergency law enacted in 1981, with a new and updated law. It will reportedly include specific measures against terrorist financing.

The United States and Egypt have a Mutual Legal Assistance Treaty. Egyptian authorities have cooperated with U.S. efforts to seek and freeze terrorist assets. The CBE circulates to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224. No related assets were identified, frozen, seized, or forfeited in 2005.

Egypt was one of the founding members the Middle East and North Africa Financial Action Task Force (MENAFATF). In November 2004, Egypt was elected to a one-year term as the first Vice-President of MENAFATF. In January 2006, it assumed the presidency for a one-year period.

Egypt is a party to the 1988 UN Drug Convention. In March 2004, it ratified the UN Convention against Transnational Organized Crime. In March 2005, it ratified the UN International Convention for the Suppression of the Financing of Terrorism.

The GOE implemented reforms in 2005 to address domestic and international concerns regarding deficiencies in its banking sector and anti-money laundering regime. However, Egypt should follow through with its plans to enact an updated law against terrorism that specifically addresses the threat of terrorist financing. The GOE must also improve its ability to pursue suspicious financial activities and transactions through the entire investigative and judicial process. It should consider ways of improving the MLCU'S feedback on STRs to reporting institutions. It should improve its enforcement of cross-border currency controls, including reporting requirements.

El Salvador

Located on the Pacific coast of the Central American isthmus, El Salvador has one of the largest and most developed banking systems in Central America. Its most significant financial contacts are with neighboring Central American countries, as well as with the United States, Mexico, and the Dominican Republic. The January 2001 adoption of the U.S. dollar as legal tender, along with the size and growth rate of the financial sector, makes the country a potentially fertile ground for money laundering. In 2005, more than $2 billion in remittances were likely sent to El Salvador through the financial system. Most were sent from Salvadorans working in the United States to family members. Additional remittances flow back to El Salvador via other methods such as visiting relatives and regular mail.

Most money laundering is conducted by international criminal organizations. These organizations use bank and wire fund transfers from the United States to disguise criminal revenues as legitimate remittances to El Salvador. The false remittances are collected and transferred to other financial institutions until sufficiently laundered for use by the source of the criminal enterprise, usually a narcotics trafficking organization.

Decree 498 of 1998, the "Law Against the Laundering of Money and Assets," criminalizes money laundering related to narcotics trafficking and other serious crimes, including trafficking in persons, kidnapping, extortion, illicit enrichment, embezzlement, and contraband. The law also establishes the financial intelligence unit (FIU) within the Attorney General's Office. The FIU has been operational since January 2000. The National Police (PNC) and the Central Bank also have their own anti-money laundering units.

Under Decree 498, financial institutions must identify their customers, maintain records for a minimum of five years, train personnel in identification of money and asset laundering, establish internal auditing procedures, and report all suspicious transactions and transactions that exceed approximately $57,000 to the FIU. Entities obligated to comply with these requirements include banks, finance companies, exchange houses, stock exchanges and exchange brokers, commodity exchanges, insurance companies, credit card companies, casinos, dealers in precious metals and stones, real estate agents, travel agencies, the postal service, construction companies, and the hotel industry. The law includes a safe harbor provision to protect all persons who report transactions and cooperate with law enforcement authorities, and also contains banker negligence provisions that make individual bankers responsible for money laundering at their institutions. Bank secrecy laws do not apply to money laundering investigations.

To address the problem of international transportation of criminal proceeds, Decree 498 requires all incoming travelers to declare the value of goods, cash, or monetary instruments they are carrying in excess of approximately $11,400. Falsehood, omission, or inaccuracy on such a declaration is grounds for retention of the goods, cash, or monetary instruments, and the initiation of criminal proceedings. If, following the end of a 30-day period, the traveler has not proved the legal origin of said property, the Salvadoran authorities have the authority to confiscate it.

The Government of El Salvador (GOES) has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related and other assets of serious crimes. The FIU and PNC have adequate police powers to trace and seize assets, but the PNC lacks the resources to do so. Even if resources were abundant, it remains to be seen if these government agencies can cooperate to achieve their anti-money laundering goals. For example, only one arrest for money laundering was achieved in 2005. The detained individual is accused of establishing wire transfer accounts in fictitious names in order to receive transfers from the United States disguised as remittances. Unfortunately, the Attorney General's Office declined to pursue several leads generated by this person's arrest. As a result, it is likely that any evidence linking others to this scheme has already been destroyed.

Forfeited money laundering proceeds are deposited in a special fund used to support law enforcement, drug treatment and prevention, and other related government programs, while funds forfeited as the result of other criminal activity are deposited into general government revenues. Law enforcement agencies are allowed to use certain seized assets while a final sentence is pending. There exists no legal mechanism to share seized assets with other countries. Salvadoran law currently provides only for the judicial forfeiture of assets upon conviction (criminal forfeiture), and not for civil or administrative forfeiture. A draft law to reform Decree 498 to provide for civil forfeiture of assets has stalled in the national legislature.

Although Decree 498 does not specifically mention terrorism or terrorist financing as predicate offenses for money laundering, it criminalizes the laundering of the proceeds of serious criminal acts. This has been interpreted to include terrorism. Therefore, it is illegal to launder money generated by a terrorist act, and assets of terrorists that are derived from criminal activities could be targeted under Decree 498. However, providing legitimate money (money that is not derived from a criminal act) to known terrorist organizations is not considered to be a crime, and the person contributing those funds could not be prosecuted unless it could be shown that he or she was directly involved in the planning or execution of a crime.

The GOES has drafted counterterrorism legislation that will further define acts of terrorism and establish tougher penalties for the execution of those acts. The draft legislation, if passed, would also grant the GOES the legal authority to freeze and seize suspected assets associated with terrorists and terrorism. The GOES has circulated the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list to financial institutions. These institutions are required to search for any assets related to the individuals and entities on the consolidated list. There is no evidence that any charitable or nonprofit entity in El Salvador has been used as a conduit for terrorist financing.

El Salvador has signed several agreements of cooperation and understanding with supervisors from other countries to facilitate the exchange of supervisory information, including permitting on-site examinations of banks and trust companies operating in El Salvador. El Salvador is a party to the Treaty of Mutual Legal Assistance in Criminal Matters signed by the Republics of Costa Rica, Honduras, Guatemala, Nicaragua, and Panama. Salvadoran law does not require the FIU to sign agreements in order to share or provide information to other countries. The GOES is party to the Inter-American Convention on Mutual Assistance in Criminal Matters, which provides for parties to cooperate in tracking and seizing assets. The FIU is also legally authorized to access the databases of public or private entities. The GOES has cooperated with foreign governments in financial investigations related to narcotics, money laundering, terrorism, terrorism financing, and other serious crimes.

El Salvador is a member of the OAS Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD), the Caribbean Financial Action Task Force, and the Egmont Group. The GOES is party to the OAS Inter-American Convention Against Terrorism and the UN International Convention for the Suppression of the Financing of Terrorism, as well as the 1988 UN Drug Convention. El Salvador ratified the UN Convention against Transnational Organized Crime and the UN Convention Against Corruption in March and July of 2004, respectively. El Salvador is also a signatory to the Central American Convention for the Prevention and Repression of Money Laundering Crimes Related to Illicit Drug Trafficking and Related Crimes.

The growth of El Salvador's financial sector, the increase in narcotics trafficking, the large volume of remittances and the use of the U.S. dollar as legal tender make El Salvador vulnerable to money laundering. El Salvador should continue to expand and enhance its anti-money laundering policies and strengthen its ability to seize and share assets. Remittances are an important sector of the economy, which must therefore be carefully supervised. The Government of El Salvador should criminalize the support and financing of terrorists and terrorist organizations.

Ethiopia

Due primarily to its archaic financial systems and pervasive government controls, Ethiopia is not considered a regional financial center. There is no offshore sector. Ethiopia's location within the Horn of Africa region makes it vulnerable to money laundering related activities perpetrated by transnational criminal organizations, terrorists, and narcotics trafficking organizations. Sources of illegal proceeds include narcotics trafficking, smuggling, trafficking in persons, arms trafficking, trafficking of animal products, and corruption. Since government foreign exchange controls limit possession of foreign currency, most of the proceeds of contraband smuggling and other crimes are not laundered through the official banking system. High tariffs also encourage customs fraud and trade-related money laundering.

Historically, money laundering has not been a serious problem. However, while reliable data is not available, reportedly incidents of money laundering have increased in the past few years. Lack of data and systematic study make it difficult for the Federal Police to identify trends in money laundering and inadequate police training hampers their investigative abilities. Reports indicate that alternative remittance systems, particularly hawala, are also widely used by immigrant communities. The government has closed a number of illegal hawala operations.

Article 684 of Ethiopia's new Criminal Code, approved in May 2005, criminalizes money laundering. Under Article 684 (1), an offender could be criminally liable either for both the predicate acts and money laundering offenses or for the principal criminal act. A violation under Article 684(1) is punishable with five to fifteen years imprisonment and a fine not exceeding the equivalent of $11,560. The Central Bank has drafted separate anti-money laundering legislation, with includes a provision mandating the establishment of a Financial Intelligence Unit (FIU). This legislation is currently being reviewed by relevant government agencies. In conjunction with the UN Office on Drugs and Crime, the Government of Ethiopia is working on the development of a country strategy to help Ethiopia better respond to financial crimes. The plan includes the identification of training and capacity-building activities needed by the Ethiopian authorities, including judges and prosecutors.

The country has an underdeveloped financial infrastructure, containing six small private banks and three government banks. Currently, there are no foreign banks that operate within the country. The Central Bank has mandated that banks report suspicious transactions, but supervision capability is limited, as most records and communications are not yet computerized. Foreign exchange controls limit possession of foreign currency, and the government controls the exchange of foreign currency into local currency. There are no money laundering controls applicable to non-banking financial institutions or intermediaries. The Government of Ethiopia (GOE) has proposed counterterrorism legislation, which is still under review in Parliament. The Central Bank has the authority to identify, freeze, and seize terrorist finance related assets, and it has done so in the past. The Central Bank routinely circulates to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list. During 2005, no assets linked to these persons or entities have been identified.

Ethiopia is a party to the 1988 UN Drug Convention. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. It has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Ethiopia should act on the pending terrorist legislation and pass anti-money laundering legislation that adheres to international standards. Ethiopia should proceed with ratification of the UN Convention against Transnational Organized Crime. It should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

France

France remains an attractive venue for money laundering because of its sizable economy, political stability, and sophisticated financial system. Common methods of laundering money in France include the use of bank deposits; foreign currency and gold bullion transactions; corporate transactions; and purchases of real estate, hotels, and works of art. A 2002 Parliamentary Report states that, increasingly, Russian and Italian organized crime networks are using the French Riviera to launder assets (or invest previously laundered assets) by buying up real estate, "a welcoming ground for foreign capital of criminal origin." The report estimates that between seven and 60 billion euros of dirty money have already been channeled through the Riviera.

The Government of France (GOF) first criminalized money laundering related to narcotics trafficking in 1987 (Article L-627 of the Public Health Code). In 1988, the Customs Code was amended to incorporate financial dealings with money launderers as a crime. In 1996 the criminalization of money laundering was expanded to cover the proceeds of all crimes. In January 2004, the French Supreme Court judged that joint prosecution of individuals was possible on both money laundering charges and the underlying predicate offense. Prior to this judgment, the money laundering charge and the predicate offense were considered the same offense and could only be prosecuted as one offense.

In 1990, the obligation for financial institutions to combat money laundering came into effect with the adoption of the Monetary and Financial Code (MFC), and France's ratification of the 1988 UN Drug Convention. The 1996 amendment to the law also obligates insurance brokers to report suspicious transactions. In 1998, the covered parties were expanded to include non-financial professions (persons who carry out, verify or give advice on transactions involving the purchase, sale, conveyance or rental of real property). In 2001, the list of professions subject to suspicious transaction reporting requirements expanded to include legal representatives; casino managers; and persons customarily dealing in or organizing the sale of precious stones, precious materials, antiques, or works of art. Following the 2001 amendments, the law covers banks, moneychangers, public financial institutions, estate agents, insurance companies, investment firms, mutual insurers, casinos, notaries, and auctioneers and dealers in high-value goods. In 2004, the list was expanded again to include chartered accountants; statutory auditors; notaries; bailiffs; judicial trustees and liquidators; lawyers; judicial auctioneers and movable auction houses; groups, clubs, and companies organizing games of chance: lotteries, bets, sports and horse-racing forecasts; institutions/unions of pensions management and intermediaries entitled to handle securities.

As a member of the European Union (EU), France is obligated to implement all three EU money laundering directives, including the revision of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering (Directive 2001/97/EC), that was transposed into domestic French legislation in 2004. The EU adopted the Third Money Laundering Directive (2005/60/EC) in late 2005, and must be implemented in France by December 15, 2007.

Decree No. 2002-770 of May 3, 2002, addresses the functioning of France's Liaison Committee against the Laundering of the Proceeds of Crime. This committee is co-chaired by the French Financial Intelligence Unit (FIU), TRACFIN (the unit for Treatment of Intelligence and Action Against Clandestine Financial Circuits), and the Justice Ministry. It comprises representatives from reporting professions and institutions, regulators, and law enforcement authorities; its purpose is to supply professions required to report suspicious transactions with better information and to make proposals in order to improve the anti-money laundering system.

The Banking Commission supervises financial institutions and conducts regular audits of credit institutions, and the Insurance and Provident Institutions Supervision Commission reviews insurance brokers. The Financial Market Authority evolved from the merger of the Securities Exchange Commission and the Financial Markets Council, and monitors the reporting compliance of the stock exchange and other non-bank financial institutions. The Central Bank (Banque de France) oversees management of the required records to monitor banking transactions, such as for means of payments (checks and ATM cards), or extensions of credit. Bank regulators and law enforcement also can access the system (FICOBA) managed by the French Tax Administration for opening and closing of accounts, which covers depository accounts, transferable securities, and other properties including cash assets that are registered in France. These records are important tools in the French arsenal for combating money laundering and terrorism financing.

TRACFIN is responsible for analyzing suspicious transaction reports (STRs) that are filed by French financial institutions and non-financial professions. TRACFIN is a part of FINATER, a group created within the French Ministry of the Economy, Finance, and Industry in September 2001, in order to gather information to fight terrorist financing. The French FIU may exchange information with foreign counterparts that observe similar rules regarding reciprocity and confidentiality of information. TRACFIN works closely with the Ministry of Interior's Central Office for Major Financial Crimes (OCRGDF), which is the main point of contact for Interpol and Europol in France.

TRACFIN received 3,598 STRs in 2001, 6,896 STRs in 2002, 9,007 STRs in 2003, and 10,842 in 2004. Approximately 83 percent of STRs are sent from the banking sector. A total of 226 cases were referred to the judicial authorities in 2001, which resulted in 59 convictions of money laundering; 291 cases were referred in 2002, which resulted in 57 criminal convictions, 308 cases were referred in 2003, which resulted in 63 convictions, and 347 cases were referred in 2004.

Two other types of reports are required to be filed with the FIU. A report must be filed with TRACFIN (no threshold limit), when the identity of the principal or beneficiary remains doubtful despite due diligence. In addition, a report must be filed in cases where transactions are carried out on behalf of a third party natural person or legal entity (including their subsidiaries or establishments) by a financial entity acting in the form, or on behalf, of a trust fund or any other asset management instrument, when legal or beneficial owners are not known. The reporting obligation can also be extended by decree to transactions carried out by financial entities, on their own behalf or on behalf of third parties, with natural or legal persons, including their subsidiaries or establishments that are domiciled, registered, or established in any country or territory included on the FATF list of Non-Cooperative Countries or Territories (NCCT).

Since 1986, French counter terrorist legislation has provided for the prosecution of those involved in the financing of terrorism under the more severe offense of complicity in the act of terrorism. However, in order to strengthen this provision, the Act of November 15, 2001, introduced several new characterizations of offenses, specifically including the financing of terrorism. The offense of financing terrorist activities (art. 41-2-2 of the Penal Code) is defined according to the UN International Convention for the Suppression of the Financing of Terrorism and is subject to ten years' imprisonment and a fine of 228,600 euros. The Act also includes money laundering as an offense in connection with terrorist activity (article 421-1-6 Penal Code), punishable by ten years' imprisonment and a fine of 62,000 euros. In March 2004, the GOF passed a law that extends the scope of STR to terrorist financing.

An additional penalty of confiscation of the total assets of the terrorist offender has also been implemented. Accounts and financial assets can be frozen through both administrative and judicial measures. In 2005, the GOF moved to strengthen France's antiterrorism legal arsenal with a bill authorizing video surveillance of public places, especially nuclear and industrial sites, as well as airports and railway stations. The bill requires telephone operators and Internet café owners to keep extensive records, allows greater government access to e-communications, and allows flight passenger lists and identification information to become accessible to counterterrorism officials. It stiffens prison sentences for directing a terrorist enterprise to 30 years, and extends the possible period of detention without charge. The bill permits increased surveillance of potential targets of terrorism. It empowers the Minister of the Economy to freeze the funds, financial instruments and economic resources belonging to individuals committing or attempting to commit acts of terrorism, or to companies directly or indirectly controlled by these individuals. By granting explicit national authority to freeze assets, the bill plugs up a potential loophole concerning the freezing of citizen versus resident EU-member assets. It was passed by both chambers of Parliament in December 2005 and only requires review by the Constitutional Council before publication and entry into force.

French authorities moved rapidly to freeze financial assets of organizations associated with al-Qaida and the Taliban under UNSCR 1267. France takes actions against non-Taliban and non-al-Qaida-related groups in the context of the EU-wide "clearinghouse" procedure. Within the Group of Eight, which France chaired in 2003, France has sought to support and expand efforts targeting terrorist financing. Bilaterally, France has worked to improve the capabilities of its African partners in targeting terrorist financing, by offering technical assistance. On the operational level, French law enforcement cooperation targeting terrorist financing continues to be good.

The United States and France have entered into a Mutual Legal Assistance Treaty (MLAT), which came into force in 2001. Through MLAT requests and by other means, the French have provided large amounts of data to the United States in connection with terrorist financing. TRACFIN is a member of the Egmont Group and is the Egmont Committee Chair of the newly created Operational Working Group. TRACFIN has information-sharing agreements with 27 FIUs, and opened negotiations in 2004 for information-sharing agreements with Argentina, Bulgaria, Chile, Germany, Japan, Jersey, Liechtenstein, Mauritius, and Thailand.

France is a member of the FATF, and held the FATF Presidency for a one-year term during 2004-05. It is also a Cooperating and Supporting Nation to the Caribbean Financial Action Task Force, as well as a Supporting Observer to the Financial Action Task Force of South America Against Money Laundering (GAFISUD). France is a party to the 1988 UN Drug Convention; the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the UN Convention against Transnational Organized Crime; and the UN International Convention for the Suppression of the Financing of Terrorism. In July 2005, France ratified the UN Convention against Corruption.

The Government of France has established a comprehensive anti-money laundering regime. France should continue its active participation in international organizations to combat the domestic and global threats of money laundering and terrorist financing.

Germany

Germany has one of the largest financial centers in Europe, and German authorities have taken several steps in recent years to diminish the risks of money laundering and terrorism financing. Germany is not a major drug trafficking country, nor is it an offshore financial center. Most money laundering in Germany is related to white collar crime, but Eastern European and Turkish crime groups and narcotics traffickers launder their illicit proceeds in Germany. About three-fourths of the suspicious activity reports filed in Germany cite suspected fraud, forgery and tax evasion, according to the German financial intelligence unit's 2004 annual report.

Germany's legislation has fully incorporated the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering and takes active measures to combat terrorist financing. In 2002, the Government of Germany (GOG) enacted a number of laws to improve authorities' ability to combat money laundering and terrorist financing. These 2002 measures brought German laws into line with the first and second European Union money laundering directives (Directive 1991/308/EEC on The Prevention of The Use of The Financial System for The Purpose of Money Laundering, as revised by Directive 2001/97/EC). Germany's Money Laundering Act, amended by the Act on the Improvement of the Suppression of Money Laundering and Combating the Financing of Terrorism of August 8, 2002, criminalizes money laundering related to narcotics trafficking, fraud, forgery, embezzlement, and membership in a terrorist organization. It also increases due diligence and reporting requirements for banks and financial institutions, and requires financial institutions to obtain customer identification for transactions conducted in cash or precious metals exceeding 15,000 euros (approximately $17,800). The legislation also calls for stiffer background checks for owners of financial institutions and tighter rules for credit card companies. Banks must report suspected money laundering to the financial intelligence unit within the Federal Criminal Investigative Service (Bundeskriminalamt or BKA), as well as to the State Attorney (Staatsanwaltschaft), who can order a freeze of the account in question.

The first and second EU money laundering directives, which Germany's 2002 amendments incorporated, mandate that member states standardize and expand suspicious activity reporting requirements to include information from notaries, accountants, tax consultants, casinos, luxury item retailers, and attorneys. Since 1998, the GOG has licensed and supervised money transmitters, has shut down thousands of unlicensed money remitters, and has issued anti-money laundering guidelines to the industry. A 1998 German law requires individuals to declare when they are entering, departing, or transiting the country with over 15,000 euros (approximately $17,800) in cash. A new EU-wide law expected to take effect in June 2007 will lower this amount to 10,000 (approximately $11,850) euros.

In May 2002, the German banking, securities, and insurance industry regulators were merged into a single financial sector regulator known as the Federal Financial Supervisory Authority (BaFIN). Germany's anti-money laundering legislation requires the BaFIN to compile a centralized register of all bank accounts in Germany, including 300 million deposit accounts. As a result, in 2003, the BaFIN established a central database, which has electronic access to all key account data held by banks in Germany. Banks cooperate with authorities and use computer-aided systems to analyze their customers and their financial dealings to identify suspicious activity. Many of Germany's banks have independently developed risk assessment software to screen potential and existing clients and to monitor transactions for suspicious activity. In 2002, Germany established a single, centralized, federal financial intelligence unit (FIU) within the Federal Criminal Police. The FIU functions as an administrative unit and is staffed with financial market supervision, customs, and legal experts. The FIU is responsible for developing a central database for analyzing cases and responding to reports of suspicious transactions. Another unit under the Federal Criminal Investigative Service, the Federal Financial Crimes Investigation Task Force, has 20 Federal Criminal Investigative Service officers and customs agents. Germany plans to add seven or eight more investigators to the task force in 2006.

In 2004, more than 8,000 suspicious activity reports (SARs) were submitted to the FIU. Over one-third of the persons cited in Germany's SARs were non-German nationals. Eighty-five percent of the reports resulted in further investigative proceedings. As with other crimes, actual enforcement under the German federal system is carried out at the state (sub-federal) level. Each state has a joint customs/police/financial investigations unit (GFG), which works closely with the federal FIU. In 2003, the last year that data is available, the number of money laundering convictions totaled 128. U.S. authorities have conducted joint investigations with GFGs on a number of transnational cases.

BaFIN's system allows for immediate identification of financial assets for potential freezes. In cases where law enforcement authorities seize assets for evidentiary purposes, German law requires a direct link to the crime before seizures are allowed. Law enforcement authorities can freeze accounts for up to nine months, but the money cannot be seized until it is proven in court that the funds were derived from criminal activity or intended for terrorist activity. UN sanctions are an exception to the rule, and Germany freezes indefinitely the assets of anyone appearing on a UN list. In the first nine months of 2005, only $12,000 had been found and frozen in connection with names appearing on the UNSCR 1267 consolidated list. Proceeds from asset seizures and forfeitures are paid into the government treasury. German authorities cooperate with U.S. authorities to trace and seize assets to the full extent that German law allows. The GOG investigates leads from other countries. However, German law does not allow for sharing forfeited assets with other countries.

In 2002, the GOG added terrorism and terrorist financing as a predicate offense for money laundering, as defined by Section 261 of the Federal Criminal Code. A 2002 amendment of the Criminal Code also allows for prosecution of members of terrorist organizations based outside of Germany. Previously, German authorities could only prosecute a member of a foreign-based terrorist organization if that group had some organized presence within Germany.

The GOG moved quickly after September 11, 2001, to identify and correct weaknesses in Germany's laws that permitted terrorists to live and study in Germany prior to that date. The first reform package closed loopholes in German law that permitted members of foreign terrorist organizations to raise money in Germany, e.g., through charitable organizations, and extremists to advocate violence in the name of religion. Germany has stepped up its legislative and law enforcement efforts to prevent the misuse of charitable entities. Germany has used its Law on Associations (Vereinsgesetz) to ban by administrative action extremist associations that threaten the constitutional order.

The second reform package, which went into effect January 1, 2002, enhances the capabilities of federal law enforcement agencies, and improves the ability of intelligence and law enforcement authorities to coordinate their efforts and to share information on suspected terrorists. The new law provides Germany's internal intelligence service with access to information from banks and financial institutions, postal service providers, airlines, and telecommunication and Internet service providers.

Germany is an active participant in UN and EU processes to monitor and freeze the assets of terrorists and possesses the regulatory and legislative framework to identify and freeze rapidly the assets of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and those designated by the EU, and/or German authorities. A November 2003 amendment to the Banking Act creates a broad legal basis for the BaFIN to order freezing of assets of suspected terrorists who are EU residents. The EU Council continually updates, reviews, and issues revised lists, and Germany adheres to these lists and ensures their circulation to financial institutions. Germany and several other EU member states have taken the view that the EU Council Common Position 2001/931/CSFP requires at a minimum a criminal investigation to establish a sufficient legal basis for freezes under the EU Clearinghouse process. Germany loosened this stance in 2005 when it sought and obtained an EU asset freeze for a German association that the German Federal Interior Ministry had banned.

The GOG has responded quickly to freeze over 30 accounts of entities associated with terrorists. After September 11, 2001, Germany froze many millions of euros of Taliban-era Afghan assets, but these accounts have been unfrozen and made available to the new Government of Afghanistan.

Germany considers informal money transfer schemes, such as "*hawala*," to be banking activities. Accordingly, German authorities require banking licenses for money transfer services, allowing them to prosecute unlicensed operations and to maintain close surveillance over authorized transfer agents. The BaFIN has investigated more than 2,500 cases of unauthorized financial services since 2003. There are 47 legally licensed money transfer services.

Germany, as a member of the EU, is legally bound to implement a recent EU regulation requiring accurate originator information on funds transfers—but only for transfers into or out of the EU, not within the EU. FATF Special Recommendation Seven on Terrorist Financing, governing wire transfers, however, requires such information on all cross-national-border transfers, including intra-EU transfers.

A new immigration law that went into effect in January 2005 complements counterterrorism laws. It contains provisions designed to facilitate deporting foreigners who support terrorist organizations. Furthermore, a third counterterrorism package is currently under discussion within the government

Germany continues to be an active partner in the fight against money laundering and participates actively in a number of international fora. The FIU exchanges information with its counterparts in other countries. The GOG exchanges information with the United States through bilateral law enforcement agreements and other informal mechanisms. German law enforcement authorities also cooperate closely at the EU level, such as through Europol. Germany also has Mutual Legal Assistance Treaties (MLATs) with numerous countries. Germany and the United States signed a MLAT in October 2003. At the beginning of 2006, the U.S.-German MLAT was before the German Bundestag and the U.S. Senate for ratification. In addition, the U.S.-EU Agreements on Mutual Legal Assistance and Extradition are expected to improve further U.S.-German legal cooperation. Negotiations for the bilateral instrument to implement the treaty are complete; the document is currently awaiting signature.

Germany is a member of the FATF, the EU, the Council of Europe, and in 2003 became a member of the Egmont Group. Germany is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. Germany signed, but has not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. After signing the UN International Convention for the Suppression of the Financing of Terrorism in 2000, Germany ratified the instrument, effective July 17, 2004.

The Government of Germany's new anti-money laundering laws and its ratification of international instruments underline Germany's commitment to combat money laundering and to cooperate with the international community. Germany should continue to enhance its anti-money laundering regime and continue its active participation in international fora. It should ratify the UN Convention against Transnational Organized Crime.

Gibraltar

Gibraltar is a largely self-governing overseas territory of the United Kingdom (UK), which assumes responsibility for Gibraltar's defense and international affairs. As part of the European Union (EU), Gibraltar is required to implement all relevant EU directives, including those relating to anti-money laundering.

The Drug Offenses Ordinance (DOO) of 1995 and Criminal Justice Ordinance of 1995 criminalize money laundering related to all crimes, and mandate reporting of suspicious transactions by any person who becomes concerned about the possibility of money laundering. The DOO covers such entities as banks, mutual savings companies, insurance companies, financial consultants, postal services, exchange bureaus, attorneys, accountants, financial regulatory agencies, unions, casinos, charities, lotteries, car dealerships, yacht brokers, company formation agents, dealers in gold bullion, and political parties.

Gibraltar was one of the first jurisdictions to introduce and implement money laundering legislation that covered all crimes. The Gibraltar Criminal Justice Ordinance to Combat Money Laundering, which related to all crimes, entered into effect in 1996. Comprehensive anti-money laundering Guidance Notes (which have the force of law) were also issued to clarify the obligations of Gibraltar's financial service providers.

The Financial Services Commission (FSC) is responsible for regulating and supervising Gibraltar's financial services industry. It is required by statute to match UK supervisory standards. Both onshore and offshore banks are subject to the same legal and supervisory requirements. All relevant financial records are required to be retained for at least five years from the date of completion of the business. If the obligated institution has submitted a Suspicious Activity Report to the Gibraltar financial intelligence unit (FIU) or when it knows that a client or transaction is under investigation, it is required to maintain any relevant record even if the five year limit has been reached. If the law enforcement agency investigating a money laundering case cannot link the funds passing through the financial system with the original criminal money, then the funds cannot be confiscated.

The FSC also licenses and regulates the activities of trust and company management services, insurance companies, and collective investment schemes. Internet gaming is permitted by the Government of Gibraltar (GOG), and is subject to a licensing regime. Gibraltar has guidelines for correspondent banking, politically exposed persons, bearer securities, and "know your customer" procedures, and, has implemented the FATF Special Recommendations on Terrorist Financing.

The 2001 Terrorism (United Nations Measures) (Overseas Territories) Order makes the financing of terrorism a criminal offence. The Order requires a bank to report to the Governor, where it knows or suspects that a person is or has been a customer of that institution or with whom the institution has had dealings with is a terrorist, or a person who receives funds in relation to terrorism or makes funds available for terrorism.

In 1996, Gibraltar established the Gibraltar Coordinating Center for Criminal Intelligence and Drugs (GCID) to receive, analyze, and disseminate information on financial disclosures filed by institutions covered by the provisions of Gibraltar's anti-money laundering legislation. The GCID serves as Gibraltar's FIU and is a sub-unit of the Gibraltar Criminal Intelligence Department. The GCID consists mainly of police and customs officers but is independent of law enforcement.

In 2003, the GOG adopted and implemented the European Union Money Laundering Directive 91/308/EEC on the Prevention of the Use of the Financial System for the Purpose of Money Laundering. The GOG has implemented the 1988 UN Drug Convention pursuant to its Schengen obligations. However, the Convention has not yet been extended to Gibraltar by the United Kingdom. The Mutual Legal Assistance Treaty between the United States and the United Kingdom also has not been extended to Gibraltar. However, application of a 1988 U.S.-UK agreement concerning the investigation of drug-trafficking offenses and the seizure and forfeiture of proceeds and instrumentalities of drug-trafficking was extended to Gibraltar in 1992. Also, the DOO of 1995 provides for mutual legal assistance with foreign jurisdictions on matters related to narcotics trafficking and related proceeds. Gibraltar has passed legislation as part of the EU decision on its participation in certain parts of the Schengen arrangements, to update mutual legal assistance arrangements with the EU and Council of Europe partners. Gibraltar is a member of the Offshore

Group of Banking Supervisors (OGBS); and, in 2004, the GCID became a member of the Egmont Group.

The Government of Gibraltar should continue its efforts to implement a comprehensive anti-money laundering regime capable of thwarting terrorist financing. Gibraltar should put in place reporting requirements for cross-border currency movements.

Greece

While not a major financial center, Greece is vulnerable to money laundering related to narcotics trafficking, prostitution, contraband cigarette smuggling, and illicit gambling activities conducted by criminal organizations originating in former constituent republics of the Soviet Union, as well as in Albania, Bulgaria, Romania, and other Balkan countries. Money laundering in Greece is controlled by organized local criminal elements associated with narcotics trafficking, and narcotics are a primary source of laundered funds. Most of the funds are not laundered through the banking system. Rather, they are most commonly invested in real estate, hotels, and consumer goods such as automobiles. Implementation of regulatory requirements documenting the flow of large sums of cash through financial and other institutions—such as Greece's five private and two state-owned casinos—is weak. The cross-border movement of illicit currency and monetary instruments is a continuing problem.

Greece is not considered an offshore financial center, and there are no offshore financial institutions or international business companies (IBCs) operating within Greece. However, Greek law allows banking authorities to check transactions of companies established within Greece with offshore operations elsewhere. Senior Government of Greece (GOG) officials are not known to engage in or facilitate money laundering. Reportedly, currency transactions involving international narcotics trafficking proceeds are not believed to include significant amounts of U.S. currency.

Greece has three free trade zones, located at the ports of Piraeus, Thessalonica, and Heraklion, where foreign goods may be brought in without payment of customs duties or other taxes if they are subsequently transshipped or re-exported. There is no indication that these zones are being used in trade-based money laundering or in the financing of terrorism.

The GOG criminalizes money laundering derived from all crimes in the 1995 Law 2331/1995. That law, "Prevention of and Combating the Legalization of Income Derived from Criminal Activities," imposes a penalty for money laundering of up to ten years in prison and confiscation of the criminally derived assets. The law also requires that banks and non-bank financial institutions file suspicious transaction reports (STRs). Legislation passed in March 2001 targets organized crime by making money laundering a criminal offense when the property holdings being laundered are obtained through criminal activity or cooperation in criminal activity. Money laundering became an offense in Greece under Presidential Decree 2181/93.

In 2003 Greece enacted legislation (Law 3148) that incorporates European Union (EU) provisions in directives dealing with the operation of credit institutions and the operation and supervision of electronic money transfers. Under this legislation, the Bank of Greece has direct scrutiny and control over transactions by credit institutions and entities involved in providing services for fund transfers. The Bank of Greece issues operating licenses after a thorough check of the institutions, their management, and their capacity to ensure the transparency of transactions.

Law 3259/August 2004 allows individuals and legal entities that pay taxes in Greece to repatriate capital from any bank account held outside Greece by paying a three percent tax on the transferred funds within six months (later extended to nine months). The Bank of Greece, the nation's Central Bank, has issued a circular to financial institutions that receive repatriated funds, instructing them on how to scrutinize the transfers for possible money laundering. The Ministry of Economy and Finance has issued detailed instructions on the documentation and auditing procedures required for repatriating capital. According to the Bank of Greece, about 500 million euros have actually been transferred back to Greece under this law, considerably less than anticipated.

In November 2005, the GOG enacted new legislation that revised Law 2331/1995 to bring it in line with European Union (EU) Directive 2001/97/EC (EU Second Money Laundering Directive). The new law, 3424/2005, extends the predicate offenses for money laundering to include terrorist financing, trafficking in persons, electronic fraud, and stock market manipulation. It also extends the suspicious transaction reporting (STR) requirement to include more professionals such as auction dealers and accountants. In addition, it broadens the powers of the supervisory authorities and clarifies previous legislation by ending a conflict between confidentiality rules and anti-money laundering regulations imposed on banks and other financial institutions. The law also provides supervisory authorities with greater authority to block transactions where money laundering is suspected.

The Bank of Greece (through its Banking Supervision Department), the Ministry of National Economy and Finance (which supervises the Capital Market Commission), and the Ministry of Development (through its Directorate of Insurance Companies) supervise and closely monitor credit and financial institutions. Supervision includes the issuance of guidelines and circulars, as well as on-site examinations aimed at checking compliance with anti-money laundering legislation. Supervised institutions must send to their competent authority a description of the internal control and communications procedures they have implemented to prevent money laundering. In addition, banks must undergo internal audits. Bureaux de change are required to send to the Bank of Greece a monthly report on their daily purchases and sales of foreign currency.

Under Decree 2181/93, banks in Greece must demand customer identification information when opening an account or conducting transactions that exceed 15,000 euros. If there is suspicion of illegal activities, banks can take reasonable measures to gather more information on the identification of the person. Greek citizens must provide a tax registration number if they conduct foreign currency exchanges of 1,000 euros or more, and must provide full identification, including the name of the recipient, in exchanges involving 12,500 euros (approximately $18,050) or more. Banks and financial institutions are required to maintain adequate records and supporting documents for at least five years after ending a relationship with a customer, or, in the case of occasional transactions, for five years after the date of the transaction.

Every bank and credit institution is required by law to appoint an officer to who all other bank officers and employees must report any transaction they consider suspicious. Reporting obligations also apply to government employees involved in auditing, including employees of the Bank of Greece, the Ministry of Economy and Finance, and the Capital Markets Commission. Reporting individuals are required to furnish all relevant information to the prosecuting authorities. Reporting individuals are protected by law.

Greece has adopted banker negligence laws under which individual bankers may be held liable if their institutions launder money. Banks and credit institutions are subject to heavy fines if they breach their obligations to report instances of money laundering; bank officers are subject to fines and a prison term of up to two years. In November 2005, the Bank of Greece announced that so far in 2005, it had imposed fines totaling 8.8 million euros against 13 credit institutions and seven *bureaux de change* and had revoked the license of one *bureau de change* for violations of anti-money laundering laws. The Bank had imposed similar fines and administrative sanctions, including prohibiting the opening of new branches, in previous years as well. There have been no objections from banking and political groups to the GOG's policies and laws on money laundering.

All persons entering or leaving Greece must declare to the authorities any amount they are carrying over 2,000 euros (approximately $2,400). Reportedly, however, cross-border currency reporting requirements are not uniformly enforced at all border checkpoints.

Law 2331/1995 establishes the Competent Committee (CC) to receive and analyze STRs and to function as Greece's financial intelligence unit (FIU). The CC is chaired by a senior judge and includes representatives from the Bank of Greece, the nation's Central Bank; various government ministries; and the stock exchange. If the CC believes that an STR warrants further investigation, it forwards the STR to the Financial Crimes Enforcement Unit, a multi-agency group that functions as the CC's investigative arm. In 2004, the Financial Crimes Enforcement Unit was renamed the Special Control Directorate (YPEE) and placed under the direct supervision of the Ministry of Economy and Finance. The CC is also responsible for preparing money laundering cases on behalf of the Public Prosecutor's Office.

Law 3424 passed in November 2005 upgrades the CC to an independent authority with access to public and private files, with no tax confidentiality restrictions. The law also broadens the CC's authority in the evaluation of information it receives from various organizations within Greece as well as from international organizations. The Committee is now authorized to block suspects' funds and to impose penalties on those who fail to report suspicious transactions. It must also provide feedback to banks by informing them of actions taken with regard to STRS, in order to enhance continuity. There have been several arrests for money laundering since January 2002. These involved the Greek owners (and their spouses) of vessels transporting cocaine from Colombia and other Western Hemisphere countries. The guilty parties received five-year sentences.

With regard to the freezing of accounts and assets, Law 3424/2005 harmonizes Greece's laws with relevant EU legislation. It incorporates elements of the EU Framework Decision on the freezing of funds and other financial assets, as well as the EU Council Regulation on the financing of terrorism. The GOG says it will promulgate implementing regulations to Law 3424/2005 in the first quarter of 2006. YPEE has established a mechanism for identifying, tracing, freezing, seizing, and forfeiting assets of narcotics-related and other serious crimes, the proceeds of which are turned over to the GOG. According to the 1995 law, all property and assets used in connection with criminal activities are seized and confiscated by the GOG following a guilty verdict. Legitimate businesses can be seized if used to launder drug money. The GOG has not enacted laws for sharing seized narcotics-related assets with other governments.

In March 2001, the Ministry of Justice unveiled legislation on combating terrorism, organized crime, money laundering, and corruption. Parliament passed the legislation in July 2002. Under a new counterterrorism law (Law 3251/July 2004), anyone who provides financial support to a terrorist organization faces imprisonment of up to ten years. If a private legal entity is implicated in terrorist financing, it faces fines of between 20,000 and 3 million euros (approximately $24,070 and $3,610,000), closure for a period of two months to two years, and ineligibility for state subsidies. The law incorporates the first eight of the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing, and Law 3424/2005 completes the process by revising the old law. According to the GOG, it plans to adopt FATF's Special Recommendation Nine on cash couriers at a later date, following the issuance of a relevant EU directive.

The Bank of Greece and the Ministry of National Economy and Finance have the authority to identify, freeze, and seize terrorist assets. The Bank of Greece has circulated to all financial institutions the list of individuals and entities that have been included on the UNSCR 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Ladin, the al-Qaida organization, or the Taliban, or that the EU has designated under relevant authorities. Suspect accounts (of small amounts) have been identified and frozen.

There are no known plans on the part of the GOG to introduce legislative initiatives aimed at regulating alternative remittance systems. Illegal immigrants or individuals without valid residence permits are known to send remittances to Albania and other destinations in the form of gold and precious metals, which are often smuggled across the border in trucks and buses. The financial and economic crimes police as well as tax authorities closely monitor charitable and nongovernmental organizations; there is no evidence that such organizations are being used as conduits for the financing of terrorism.

Greece is a member of the FATF, the EU, and the Council of Europe. The CC is a member of the Egmont Group. The GOG is a party to the 1988 UN Drug Convention and in December 2000 became a signatory to the UN Convention against Transnational Organized Crime. On April 16, 2004, Greece became a party to the UN International Convention for the Suppression of the Financing of Terrorism. Greece has signed bilateral police cooperation agreements with Egypt, Albania, Armenia, France, the United States, Iran, Israel, Italy, China, Croatia, Cyprus, Lithuania, Hungary, Macedonia, Poland, Romania, Russia, Tunisia, Turkey, and Ukraine. It also has a trilateral police cooperation agreement with Bulgaria and Romania, and a bilateral agreement with Ukraine to combat terrorism, drug trafficking, organized crime, and other criminal activities.

Greece exchanges information on money laundering through its Mutual Legal Assistance Treaty (MLAT) with the United States, which entered into force November 20, 2001. The Bilateral Police Cooperation Protocol provides a mechanism for exchanging records with U.S. authorities in connection with investigations and proceedings related to narcotics trafficking, terrorism, and terrorist financing. Cooperation between the U.S. Drug Enforcement Administration and YPEE has been extensive, and the GOG has never refused to cooperate. The CC can exchange information with other FIUs, although it prefers to work with a memorandum of understanding in such exchanges.

The Government of Greece has made significant progress in expanding and adjusting its legislation to international standards by gradually incorporating all EU directives on money laundering and terrorist financing. However, in 2006 Greece must begin aggressive implementation of the legislative tools it now has at its disposal. Additionally, Greece should ensure uniform enforcement of its cross-border currency reporting requirements and take steps to deter the smuggling of precious gems and metals across its borders.

Grenada

Like many other Caribbean jurisdictions, the Government of Grenada (GOG) raises revenue from the offshore sector by imposing licensing and annual fees upon offshore entities. After being placed on the Financial Action Task Force's (FATF) list of non-cooperative countries and territories (NCCT) in the fight against money laundering in September 2001, the GOG implemented and strengthened its legislation and regulations necessary for adequate supervision of Grenada's offshore sector, which prompted the FATF to remove Grenada's name from the NCCT list in February 2003. As of November 2005, Grenada has one inactive offshore bank, one trust company, one management company, and one international insurance company. Grenada is reported to have over 20 Internet gaming sites. There are also 810 international business companies (IBCs). The domestic financial sector includes six commercial banks, 26 registered domestic insurance companies, two credit unions, and four or five money remitters. The GOG has repealed its economic citizenship legislation.

Grenada's Money Laundering Prevention Act (MLPA) of 1999 criminalizes money laundering related to offenses under the Drug Abuse (Prevention and Control) Act, whether occurring within or outside of Grenada, or other offenses occurring within or outside of Grenada, punishable by death or at least five years' imprisonment in Grenada. The MLPA also establishes a Supervisory Authority to receive, review, and forward to local authorities suspicious activity reports (SARs) from covered institutions, and imposes customer identification requirements on banking and other financial institutions. Financial institutions must report SARs to the Supervisory Authority within 14 days of the date that the transaction was determined to be suspicious. A financial institution or an employee who willfully fails to file a SAR or makes a false report is liable to criminal penalties that include imprisonment or fines up to ECD $250,000 ($93,000), and possibly revocation of the financial institution's license to operate. The Proceeds of Crime (Amendment) Act of 2003 extends anti-money laundering responsibilities to a number of non-bank financial institutions.

The Supervisory Authority issues anti-money laundering guidelines, pursuant to Section 12(g) of the MLPA, that direct financial institutions to maintain records, train staff, identify suspicious activities, and designate reporting officers. The guidelines also provide examples to help bankers recognize and report suspicious transactions. The Supervisory Authority is authorized to conduct anti-money laundering inspections and investigations. The Supervisory Authority can also conduct investigations and inquiries on behalf of foreign counterpart authorities and provide them with the results. Financial institutions could be fined for not granting access to Supervisory Authority personnel.

The Grenada International Financial Services Authority (GIFSA) monitors and regulates offshore banking. GIFSA makes written recommendations to the Minister of Finance in regard to the revocation of offshore entities' licenses and issues certificates of incorporation to IBCs. The GIFSA was brought under stricter management with an amendment to the GIFSA Act (No. 13 of 2001) that eliminated the regulator's role in marketing the offshore sector. In the future, GIFSA is expected to assume authority for regulating both onshore and offshore institutions, in some areas sharing supervision with the Eastern Caribbean Central Bank (ECCB). It is expected that GIFSA will be renamed the Grenada Authority for the Regulation of Financial Institutions. Legislation implementing the Grenada Authority for the Regulation of Financial Institutions as the new regulatory body was defeated in the Senate; however, the legislation will be reintroduced in 2006.

The International Companies Act regulates IBCs and requires registered agents to maintain records of the names and addresses of directors and beneficial owners of all shares, as well as the date the person's name was entered or deleted on the share register. Currently, there are 15 registered agents licensed by the GIFSA. There is an ECD $30,000 ($11,500) penalty, and possible revocation of the registered agent's license, for failure to maintain records. The International Companies Act also gives GIFSA the authority to conduct on-site inspections to ensure that records are being maintained on IBCs and bearer shares. GIFSA began conducting inspections in August 2002.

The International Financial Services (Miscellaneous Amendments) Act 2002 requires all offshore financial institutions to recall and cancel any issued bearer shares and to replace them with registered shares. The holders of bearer shares in non-financial institutions must lodge their bearer share certificates with a licensed registered agent. These agents are required by law to verify the identity of the beneficial owners of all shares and to maintain this information for seven years. GIFSA was given the authority to access the records and information maintained by the registered agents, and can share this information with regulatory, supervisory, and administrative agencies.

The Minister of Finance has signed a memorandum of understanding (MOU) with the ECCB that grants the ECCB oversight of the offshore banking sector in Grenada. Legislation that would incorporate the ECCB's new role into existing offshore banking legislation was adopted in 2003, but is not in effect. The ECCB will have the authority to share bank and customer information with foreign authorities. The ECCB already provides similar regulation and supervision to Grenada's domestic banking sector.

Grenada's legal framework effectively enables GIFSA to obtain customer account records from an offshore financial institution upon request, and to share the customer account information that regulated financial institutions must maintain under due diligence requirements with other regulatory, supervisory, and administrative bodies. GIFSA also has the ability to access auditors' working papers, and can share this information as well as examination reports with relevant authorities.

In June 2001, the GOG established a Financial Intelligence Unit (FIU) headed by a prosecutor from the Attorney General's office; the staff includes an assistant superintendent of police, four additional police officers, and two support personnel. In 2003, Grenada enacted an FIU Act (No. 1 of 2003). The

FIU, which operates within the police force but is assigned to the Supervisory Authority, is charged with receiving SARs from the Supervisory Authority and with investigating alleged money laundering offenses. By November 2005, the FIU had received 39 SARs, which resulted in the investigations of 29 SARs. Two arrests were made on drug-related money laundering charges, and the two cases are currently pending before the court. Approximately ECD $9,000 ($3,300) was seized in 2005. The FIU can provide information concerning SARs to any foreign FIU. Grenada has cooperated extensively with U.S. law enforcement in numerous money laundering and other financial crimes investigations. As a result, several subjects in the United States were successfully prosecuted.

In 2003, Grenada enacted counterterrorist financing (CFT) legislation, which provides authority to identify, freeze, and seize terrorist assets. The CFT legislation allows for the exchange of information with another country regardless of the existence of a mutual legal assistance treaty. The GOG circulates lists of terrorists and terrorist entities to all financial institutions in Grenada. There has been no known identified evidence of terrorist financing in Grenada. Money laundering in Grenada is primarily tied to narcotics proceeds. To date the GOG has not identified any indigenous alternative remittance systems, but suspect there are some in operation. Grenada has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and nonprofit entities.

During 2003, the GOG passed the Exchange of Information Act No. 2 of 2003, which will strengthen the GOG's ability to share information with foreign regulators. A Mutual Legal Assistance Treaty and an Extradition Treaty have been in force between Grenada and the United States since 1999. Grenada also has a Tax Information Exchange Agreement with the United States. Grenada's cooperation under the Mutual Legal Assistance Treaty has recently been excellent. Grenada also has demonstrated consistently good cooperation with the U.S. Government by responding rapidly to requests for information involving money laundering cases. Grenada is an active member of the Caribbean Financial Action Task Force (CFATF), and underwent a second CFATF mutual evaluation in September 2003. Grenada became a member of the Egmont Group in June 2004. Grenada is a member of the OAS Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering. Grenada is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime.

Although the Government of Grenada has strengthened the regulation and oversight of its financial sector, it must remain alert to potential abuses and must steadfastly implement the laws and regulations it has adopted. Grenada should also continue to enhance its information sharing, particularly with other Caribbean jurisdictions. The GOG should also move forward in adopting civil forfeiture legislation.

Guatemala

Guatemala is a major transit country for illegal narcotics from Colombia and precursor chemicals from Europe. Those factors, combined with historically weak law enforcement and judicial regimes, corruption, and increasing organized crime activity, lead authorities to suspect that significant money laundering occurs in Guatemala. According to law enforcement sources, narcotics trafficking is the primary source of money laundered in Guatemala; however, the laundering of proceeds from other illicit sources, such as human trafficking, contraband, kidnapping, tax evasion, vehicle theft, and corruption, is substantial. Officials of the Government of Guatemala (GOG) believe that couriers, offshore accounts, and wire transfers are used to launder funds, which are subsequently invested in real estate, capital goods, large commercial projects, and shell companies, or are otherwise transferred through the financial system.

Guatemala is not considered a regional financial center, but it is an offshore center. Exchange controls have largely disappeared and dollar accounts are common, but some larger banks conduct significant business through their offshore subsidiaries. The Guatemalan financial services industry is comprised of 26 commercial banks (three more in the process of liquidation); approximately 11 offshore banks (all affiliated, as required by law, with a domestic financial group); 6 licensed money exchangers (hundreds exist informally); 27 money remitters, including wire remitters and remittance-targeting courier services; 18 insurance companies; 17 financial societies (bank institutions that act as financial intermediaries specializing in investment operations); 15 bonded warehouses; 213 cooperatives, credit unions, and savings and loan institutions; 11 credit card issuers; seven leasing entities; 12 finanzas (financial guarantors); and 1 check-clearing entity run by the Central Bank.

The Superintendence of Banks (SIB), which operates under the general direction of the Monetary Board, has oversight and inspection authority over the Bank of Guatemala, as well as over banks, credit institutions, financial enterprises, securities entities, insurance companies, currency exchange houses, and other institutions as may be designated by the Bank of Guatemala Act. Guatemala's relatively small free trade zones target regional maquila (assembly line industries) and logistic center operations, and are not considered by GOG officials to be a money laundering concern; although proceeds from tax-related contraband are probably laundered through them.

The offshore financial sector initially offered a way to circumvent currency controls and other costly financial regulations. However, financial sector liberalization has largely removed many incentives for legitimate businesses to conduct offshore operations. All offshore institutions are subject to the same requirements as onshore institutions. In June 2002, Guatemala enacted the Banks and Financial Groups Law (No. 19-2002), which places offshore banks under the oversight of the SIB. The law requires offshore banks to be authorized by the Monetary Board and to maintain an affiliation with a domestic institution. It also prohibits an offshore bank that is authorized in Guatemala from doing business in another jurisdiction; however, banks authorized by other jurisdictions may do business in Guatemala under certain limited conditions.

Guatemala completed the process of reviewing and licensing its offshore banks in 2004, which included performing background checks of directors and shareholders. In order to authorize an offshore bank, the financial group to which it belongs must first be authorized, under a 2003 resolution of the Monetary Board. Eleven offshore banks have been authorized. By law, no offshore financial services businesses other than banks are allowed, but there is evidence that they exist in spite of that prohibition. In 2004, the SIB and Guatemala's financial intelligence unit, the Intendencia de Verificación Especial, concluded a process of reviewing and licensing all offshore entities, a process which resulted in the closure of two operations. No offshore trusts have been authorized, and offshore casinos and Internet gaming sites are not regulated.

There is continuing concern over the volume of money passing informally through Guatemala. Much of the more than $2.8 billion in remittance flows pass through informal channels, although sector reforms are leading to the increasing use of banks and other formal means of transmission. Implementing regulations for the recently passed terrorism finance legislation include measures to increase reporting requirements on remittance transmitters. Money seized at the airports, approximately $275,000 in 2005, suggest that proceeds from illicit activity are regularly hand carried over Guatemalan borders. Increasing financial sector competition should continue to expand services and bring more people into the formal banking sector, isolating those who abuse informal channels.

In June 2001, the Financial Action Task Force (FATF) placed Guatemala on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering. Since that time, authorities have implemented the necessary reforms to bring Guatemala into compliance with international standards, including the creation of a financial intelligence unit (FIU) and the passage of comprehensive anti-money laundering legislation. An inspection in May 2004 by a FATF review team found that the GOG had made excellent progress, and Guatemala was removed from the NCCT list at the FATF plenary in June 2004.

In November 2001, Guatemala enacted Decree 67-2001, the "Law Against Money and Asset Laundering," to address several of the deficiencies identified by the FATF. Article 2 of the law expands the range of predicate offenses for money laundering from drug offenses to any serious crime. Individuals convicted of money or asset laundering are subject to a non-commutable prison term ranging from six to 20 years, and fines equal to the value of the assets, instruments, or products resulting from the crime. Convicted foreigners will be expelled from Guatemala. Conspiracy and attempt to commit money laundering are also penalized.

Over time, the GOG has taken important steps to reform its anti-money laundering program. On April 25, 2001, the Guatemalan Monetary Board issued Resolution JM-191, approving the "Regulation to Prevent and Detect the Laundering of Assets" (RPDLA) submitted by the Superintendence of Banks. The RPDLA, effective May 1, 2001, requires all financial institutions under the oversight and inspection of the SIB to establish anti-money laundering measures, and introduces requirements for transaction reporting and record keeping. Covered institutions must establish money laundering detection units, designate compliance officers, and train personnel to detect suspicious transactions. The Guatemalan financial sector has largely complied with these requirements and has a generally cooperative relationship with the SIB.

Decree 67-2001 adds record keeping and transaction reporting requirements to those already in place as a result of the RPDLA. These new requirements apply to all entities under the oversight of the SIB, as well as several other entities, including credit card issuers and operators, check cashers, sellers or purchasers of travelers' checks or postal money orders, and currency exchangers. The law establishes that owners, managers, and other employees are expressly immune from criminal, civil, or administrative liability when they provide information in compliance with the law. However, it holds institutions and businesses responsible, regardless of the responsibility of owners, directors, or other employees, and they may face cancellation of their banking licenses and/or criminal charges for laundering money or allowing laundering to occur. The requirements also apply to offshore entities that are described by the law as "foreign-domiciled entities" that operate in Guatemala but are registered under the laws of another jurisdiction.

Covered institutions are prohibited from maintaining anonymous accounts or accounts that appear under fictitious or inexact names. However, non-banks may issue bearer shares, and there is limited banking secrecy. Covered entities are required to keep a registry of their customers as well as of the transactions undertaken by them, such as the opening of new accounts, the leasing of safety deposit boxes, or the execution of cash transactions exceeding approximately U.S. $10,000. Under the law, covered entities must maintain records of these registries and transactions for five years.

Decree 67-2001 also obligates individuals and legal entities to report to the competent authorities cross-border movements of currency in excess of approximately $10,000. At Guatemala City airport, a new special unit was formed in 2003 to enforce the use of customs declarations upon entry to and exit from Guatemala. Compliance is not regularly monitored at land borders.

Decree 67-2001 establishes an FIU, the Intendencia de Verificación Especial (IVE), within the Superintendence of Banks, to supervise covered financial institutions and ensure their compliance with the law. The IVE began operations in 2002 and has a staff of 26. The IVE has the authority to obtain all information related to financial, commercial, or business transactions that may be connected to money laundering. Covered entities are required to report to the IVE any suspicious transactions within 25 days of detection and to submit a comprehensive report every trimester, even if no suspicious transactions have been detected. Entities also must maintain a registry of all cash transactions exceeding approximately $10,000 or more per day, and report these transactions to the IVE.

The IVE conducts inspections on the covered entities' management, compliance officers, anti-money laundering training programs, "know-your-client" policies, and auditing programs. The IVE may impose sanctions on financial institutions for noncompliance with reporting requirements, and has imposed over $100,000 in civil penalties to date. Terrorist finance legislation passed in August 2005 requires remitters to maintain the sender's name and address information (principally U.S.-based) on transfers equal to or over an amount to be determined by implementing regulations.

Since its inception, the IVE has received approximately 1,600 suspicious transaction reports (STRs) from the 400 covered entities in Guatemala. All STRs are received electronically, and the IVE has developed a system of prioritizing them for analysis. After determining that an STR is highly suspicious, the IVE gathers further information from public records and databases, other covered entities and foreign FIUs, and assembles a case. Bank secrecy can be lifted for the investigation of money laundering crimes. Once the IVE has determined a case warrants further investigation, the case must receive the approval of the SIB before being sent to the Anti-Money or Other Assets Laundering Unit (AML Unit) within the Public Ministry. Under current regulations, the IVE cannot directly share the information it provides to the AML Unit with any other special prosecutors (principally the anticorruption or counternarcotics units) in the Public Ministry. The IVE also assists the Public Ministry by providing information upon request for other cases the prosecutors are investigating.

Sixteen cases have been referred by the IVE to the AML Unit, four of which stem from public corruption. In several cases, assets have been frozen. Nine money laundering prosecutions have been concluded, all of which resulted in a conviction. A sentence has been rendered in one case, with the remaining eight cases awaiting the completion of appeals. Additional cases have been developed with the cooperation of the Public Ministry and the IVE. The Public Ministry's AML Unit had initiated 197 cases as of December 2005. In addition, 93 cases were dismissed and 66 cases are either under continuing investigation or in initial stages of the trials, and the remaining cases were transferred to other offices for investigation and prosecution (such as the anticorruption unit) due to the nature of their particular predicate offenses. Several high profile cases of laundering proceeds from major corruption scandals involving officials of the previous government are currently under investigation and have resulted in arrests and substantial seizures of funds and assets. These seizures have been supported by the cooperating financial institutions along with the vast majority of public and political interests.

Under current legislation, any assets linked to money laundering can be seized. Within the GOG, the IVE, the National Civil Police, and the Public Ministry have the authority to trace assets; the Public Ministry can seize assets temporarily or in urgent cases; and the Courts of Justice have the authority to permanently seize assets. The GOG passed reforms in 1998 to allow the police to use narcotics traffickers' seized assets. These provisions also allow for 50 percent of the money to be used by the IVE and others involved in combating money laundering. In 2003, the Guatemalan Congress approved reforms to enable seized money to be shared among several GOG agencies. Nevertheless, the Constitutional Court ruled that forfeited currency remains under the jurisdiction of the Supreme Court of Justice.

An additional problem is that the courts do not allow seized currency to benefit enforcement agencies while cases remain open. For money laundering and narcotics cases, any seized money is deposited in a bank safe and all material evidence is sent to the warehouse of the Public Ministry. There is no central tracking system for seized assets, and it is currently impossible for the GOG to provide an accurate listing of the seized assets in custody. In 2005, Guatemalan authorities seized more than U.S. $6.5 million in bulk currency, significantly less that the $20 million seized in 2003 (although one case alone in 2003 accounted for more than $14 million). The lack of access to the resources of seized assets outside of the judiciary has made sustaining seizure levels difficult for the resource-strapped enforcement agencies.

In June 2005, the Guatemalan Congress passed antiterrorist finance legislation. Implementing regulations were submitted to the Monetary Board in December 2005. According to the GOG, Article

391 of the penal code already sanctioned all preparatory acts leading up to a crime and financing would likely be considered a preparatory act. Technically, both judges and prosecutors could have issued a freeze order on terrorist assets, but no test case ever validated these procedures. The new Terrorism Finance legislation removed potential uncertainty regarding the legality of freezing assets when no predicate offense had been legally established but the assets have been determined destined to terrorists or to support terrorist acts. The GOG has been cooperative in looking for terrorist financing funds. The new legislation is intended to bring Guatemala into compliance with the Nine FATF Special Recommendations on Terrorist Financing and the UNSCR 1373.

The SIB, through the IVE, has signed Memoranda of Understanding (MOUs) with Argentina, the Bahamas, Barbados, Bolivia, Brazil, Colombia, Costa Rica, the Dominican Republic, El Salvador, Honduras, Mexico, Montserrat, Panama, Peru, Spain and Venezuela. During 2004, the SIB signed MOUs with Belgium, France, South Korea and the United States. Guatemala signed MOUs with Albania, Saint Vincent and the Grenadines, Haiti, Bermuda, Italy, Chile, the Lesser Antilles, Lebanon, Ukraine, Romania, and Bulgaria. Guatemalan law enforcement is actively cooperating with U.S. Government law enforcement agencies on cases of mutual interest.

Guatemala is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. The GOG has signed, but not yet ratified, the UN Convention against Corruption. Guatemala is a party to the Central American Convention for the Prevention of Money Laundering and Related Crimes, and is a member of the OAS Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD) and the Caribbean Financial Action Task Force (CFATF). In 2003, the IVE became a member of the Egmont Group.

Corruption and organized crime remain strong forces in Guatemala and may prove to be the biggest hurdles facing the GOG in the long term. Guatemala has made efforts to comply with international standards and improve its anti-money laundering regime. In 2004, Guatemalan authorities completed implementation of new procedures to license and monitor offshore banks, and demonstrated that they could use anti-money laundering laws to successfully target criminals. In 2005 there was a deepening of this implementation and improvement of monitoring procedures, including expanded antiterrorism finance tools. However, Guatemala should take steps to immobilize bearer shares, and to identify and regulate offshore financial services and gaming establishments.

Guatemala should continue efforts to improve enforcement and implementation of needed reforms. Cooperation between the IVE and the Public Ministry has improved since the new administration took office in January 2004, and several investigations have led to prosecutions. However, Guatemala should continue to focus its efforts on boosting its ability to successfully investigate and prosecute money launderers and on distributing seized assets to law enforcement agencies to assist in the fight against money laundering and other financial crime.

Guernsey

The Bailiwick of Guernsey (the Bailiwick) covers a number of the Channel Islands (Guernsey, Alderney, Sark, and Herm in order of size and population). The Islands are a Crown Dependency because the United Kingdom (UK) is responsible for their defense and international relations. However, the Bailiwick is not part of the UK. Alderney and Sark have their own separate parliaments and civil law systems. Guernsey’s parliament legislates criminal law for all of the islands in the Bailiwick. The Bailiwick alone has competence to legislate in and for domestic taxation. The Bailiwick is a sophisticated financial center and, as such, it continues to be vulnerable to money laundering at the layering and integration stages.

There are approximately 16,000 companies registered in the Bailiwick. Non-residents own approximately half of the companies, and they have an exempt tax status. These companies do not fall within the standard definition of an international business company (IBC). Local residents own the remainder of the companies, including trading and private investment companies. Exempt companies are not prohibited from conducting business in the Bailiwick, but must pay taxes on profits of any business conducted on the islands. Companies can be incorporated in Guernsey and Alderney, but not in Sark, which has no company legislation. Companies in Guernsey may not be formed or acquired without disclosure of beneficial ownership to the Guernsey Financial Services Commission (the Commission).

Guernsey has 54 banks, all of which have offices, records, and a substantial presence in the Bailiwick. The banks are licensed to conduct business with residents and non-residents alike. Although total deposits into the financial institutions of the Bailiwick have remained constant, deposits from Switzerland have increased from one percent in 2003 to four percent in 2004; the increase appears to continue in 2005. There are approximately 650 international insurance companies and approximately 700 collective investment funds. There are also approximately 20 *bureaux de change*, which file accounts with the tax authorities. Many are part of a licensed bank, and it is the bank that publishes and files accounts.

Guernsey has put in place a comprehensive legal framework to counter money laundering and the financing of terrorism. The Proceeds of Crime (Bailiwick of Guernsey) Law 1999, as amended, is supplemented by the Criminal Justice Proceeds of Crime (Bailiwick of Guernsey) Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) Regulations, 2002. The legislation criminalizes money laundering for all crimes except drug-trafficking, which is covered by the Drug Trafficking (Bailiwick of Guernsey) Law, 2000. The Proceeds of Crime Law and the Regulations are supplemented by Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism, issued by the Commission. There is no exemption for fiscal offenses. The 1999 law creates a system of suspicious transaction reporting (including tax evasion) to the Guernsey Financial Intelligence Service (FIS). In 2003, Guernsey incorporated amendments to the Banking Supervision Law and began publishing the Code of Practice for Banks. The Bailiwick narcotics trafficking, anti-money laundering, and terrorism laws designate the same foreign countries as the UK to enforce foreign restraint and confiscation orders.

The Drug Trafficking (Bailiwick of Guernsey) Law 2000 consolidates and extends money laundering legislation related to narcotics trafficking. It introduces the offense of failing to disclose the knowledge or suspicion of drug money laundering. The duty to disclose extends beyond financial institutions to cover others as well, for example, bureaux de change and check cashers.

In addition, the Bailiwick authorities recently enacted the Prevention of Corruption (Bailiwick of Guernsey) Law of 2003. They have also resolved to merge existing drug trafficking, money laundering and other crimes into one statute, and to introduce a civil forfeiture law.

On April 1, 2001, the Regulation of Fiduciaries, Administration Businesses, and Company Directors, etc. (Bailiwick of Guernsey) Law of 2000 ("the Fiduciary Law") came into effect. The Fiduciary Law was enacted to license, regulate and supervise company and trust service providers. Under Section 35 of the Fiduciary Law, the Commission creates Codes of Practice for corporate service providers, trust service providers and company directors. Under the law, the Commission must license all fiduciaries, corporate service providers and persons acting as company directors of any business. In order to be licensed, these agencies must pass strict tests. These include "know your customer" requirements and the identification of clients. These organizations are subject to regular inspection, and failure to comply could result in the fiduciary being prosecuted and/or its license being revoked. The Bailiwick is fully compliant with the Offshore Group of Banking Supervisors Statement of Best Practice for Company and Trust Service Providers.

Since 1988, the Commission has regulated the Bailiwick's financial services businesses. The Commission regulates banks, insurance companies, mutual funds and other collective investment schemes, investment firms, fiduciaries, company administrators and company directors. The Bailiwick does not permit bank accounts to be opened unless there has been a "know your customer" inquiry and verification details are provided. The AML/CFT Regulations contain penalties to be applied when financial services businesses do not follow the requirements of the Regulations. Company incorporation is by act of the Royal Court, which maintains the registry. All first-time applications to form a Bailiwick company have to be made to the Commission, which then evaluates each application. The court will not permit incorporation unless the Commission and the Attorney General or Solicitor General has given prior approval. The Commission conducts regular on-site inspections and analyzes the accounts of all regulated institutions. In 2004, the Commission conducted 124 on-site inspections of financial institutions to insure compliance with the AML/CFT legislation.

On July 1, 2005, the European Union Savings Tax Directive (ESD) came into force. The ESD is an agreement between the Member States of the European Union (EU) to automatically exchange information with other Member States about EU tax resident individuals who earn income in one EU Member State but reside in another. Although not part of the EU, the three UK Crown Dependencies (Guernsey Jersey, and Isle of Man), have voluntarily agreed to apply the same measures to those in the ESD and have elected to implement the withholding tax option (also known as the "retention tax option") within the Crown Dependencies.

Under the retention tax option, each financial services provider will automatically deduct tax from interest and other savings income paid to EU resident individuals. The tax will then be submitted to local and Member States tax authorities annually. The tax authorities receive a bulk payment but do not receive personal details of individual customers. If individuals elect the exchange of information option, then no tax is deducted from their interest payments but details of the customer's identity, residence, paying agent, level and time period of savings income received by the financial services provider will be reported to local tax authorities where the account is held and then forwarded to the country where the customer resides.

The Guernsey authorities have established a forum, the Crown Dependencies Anti-Money Laundering Group, where the Attorneys General from the Crown Dependencies, Directors General and other representatives of the regulatory bodies, and representatives of police, Customs, and the FIS meet to coordinate the anti-money laundering and counterterrorism policies and strategy in the Dependencies.

The FIS operates as the Bailiwick's financial intelligence unit (FIU). The FIS began operations in April 2001, and is currently staffed by Police and Customs/Excise Officers. The FIS is directed by the Service Authority, which is a small committee of senior Police and Customs Officers who co-ordinate with the Bailiwick's financial crime strategy and report to the Chief Officers of Police and Customs/Excise. The FIS is mandated to place specific focus and priority on money laundering and terrorism financing issues. Suspicious Transaction Reports (STRs) are filed with the FIS, which is the central point within the Bailiwick for the receipt, collation, evaluation, and dissemination of all financial crime intelligence. The FIS received 777 STRs in 2002, 705 STRs in 2003, and 757 STRs in 2004.

In November 2002, the International Monetary Fund (IMF) undertook an assessment of Guernsey's compliance with internationally accepted standards and measures of good practice relative to its regulatory and supervisory arrangements for the financial sector. The IMF report states that Guernsey has a comprehensive system of financial sector regulation with a high level of compliance with international standards. As for AML/CFT, the IMF report highlights that Guernsey has a developed legal and institutional framework for AML/CFT and a high level of compliance with the FATF Recommendations.

There has been counterterrorism legislation covering the Bailiwick since 1974. The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, replicates equivalent UK legislation.

The Criminal Justice (International Cooperation) (Bailiwick of Guernsey) Law, 2000, furthers cooperation between Guernsey and other jurisdictions by allowing certain investigative information concerning financial transactions to be exchanged. Guernsey cooperates with international law enforcement on money laundering cases. In cases of serious or complex fraud, Guernsey's Attorney General can provide assistance under the Criminal Justice (Fraud Investigation) (Bailiwick of Guernsey) Law 1991. The Commission also cooperates with regulatory/supervisory and law enforcement bodies.

On September 19, 2002, the United States and Guernsey signed a Tax Information Exchange Agreement, which is not yet in force. The agreement provides for the exchange of information on a variety of tax investigations, paving the way for audits that could uncover tax evasion or money laundering activities. Currently, similar agreements are being negotiated with other countries, among them members of the European Union.

After its extension to the Bailiwick, Guernsey enacted the necessary legislation to implement the Council of Europe Convention on Mutual Assistance in Criminal Matters, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and the 1988 UN Drug Convention. The 1988 Agreement Concerning the Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking, as amended in 1994, was extended to the Bailiwick in 1996. The Bailiwick has requested that the UK Government seek the extension to the Bailiwick of the UN International Convention for the Suppression of the Financing of Terrorism.

The Attorney General's Office is represented in the European Judicial Network and has been participating in the European Union's PHARE anti-money laundering project. The Commission cooperates with regulatory/supervisory and law enforcement bodies. It is a member of the International Association of Insurance Supervisors, the Offshore Group of Insurance Supervisors, the Association of International Fraud Agencies, the International Organization of Securities Commissions, the Enlarged Contact Group for the Supervision of Collective Investment Funds, and the Offshore Group of Banking Supervisors. The FIS is a member of the Egmont Group.

Guernsey has put in place a comprehensive anti-money laundering regime, and has demonstrated its ongoing commitment to fighting financial crime. Bailiwick officials should continue both to carefully monitor Guernsey's anti-money laundering program to assure its effectiveness, and to cooperate with international anti-money laundering authorities. The Bailiwick should work with the UK to extend the UN International Convention for the Suppression of the Financing of Terrorism to Guernsey.

Guyana

Guyana is neither an important regional financial center nor an offshore financial center, nor does it have any notable offshore business sector or free trade zones. However, the scale of money laundering is thought to be large relative to the size of the economy, with some experts estimating that the informal economy is forty to sixty percent of the size of the formal sector. Money laundering has been linked to trafficking in drugs, firearms and persons, as well as corruption and fraud. Drug trafficking and money laundering appear to be propping up the Guyanese economy. Known drug traffickers have acquired substantial landholdings and timber concessions, are building large hotel and housing developments, and own retail businesses that sell imported goods at impossibly low prices. Political instability, government inefficiency, an internal security crisis, and a lack of resources have significantly impaired Guyana's efforts to bolster its anti-money laundering regime. Investigating and trying money laundering cases is not a priority for law enforcement. The Government of Guyana

(GOG) made no arrests or prosecutions for money laundering in 2005 due to lack of adequate legislation, regulations, and resources, as well as the apparent lack of political resolve to tackle money laundering as a serious crime.

The Money Laundering Prevention Act passed in 2000 is not yet fully in force, due to inadequate implementing regulations, difficulties associated with finding suitable personnel to staff the Financial Investigations Unit (FIU), and the Bank of Guyana's lack of capacity to fully execute its mandate. Crimes covered by the Money Laundering Prevention Act include narcotics trafficking, illicit trafficking of firearms, extortion, corruption, bribery, fraud, counterfeiting, and forgery. The law also requires that incoming or outgoing funds over $10,000 be reported. Licensed financial institutions are required to report suspicious transactions, although banks are left to determine thresholds individually according to banking best practices. Financial institutions must keep suspicious activity reports for seven years. The legislation also includes provisions regarding confidentiality in the reporting process, good faith reporting, penalties for destroying records related to an investigation, asset forfeiture, and international cooperation.

The Government of Guyana established a financial intelligence unit (FIU) within the Ministry of Finance in 2003. The FIU is currently staffed by a director and a police investigator. Building on assistance from U.S. funding through July 2005, the Government of Guyana (GOG) currently funds salaries and operating expenses. As of December 2005, the FIU has conducted preliminary investigations on approximately 36 cases. In addition to the FIU, government bodies responsible for investigating financial crimes include the Guyana Revenue Authority, the Customs Anti-Narcotics Unit, the Attorney General, and the Director for Public Prosecutions.

The Money Laundering Act of 2000 provides for seizure of assets derived as proceeds of crime, including money, investments, and real and personal property, but the guidelines for implementing seizures/forfeitures have not been finalized. The FIU has prepared drafts of legislation related to terrorist finance and money laundering. This more robust legislation is currently under review and is expected to be presented to parliament in spring of 2006. The new legislation is also expected to provide for oversight of export industries, real estate, and alternative remittance systems.

The Ministry of Foreign Affairs and the Bank of Guyana (the Central Bank), continue to assist U.S. efforts to combat terrorist financing by working towards coming into compliance with relevant United Nations Security Council Resolutions (UNSCRs). In 2001 the Bank of Guyana, the sole financial regulator as designated by the Financial Institutions Act of March 1995, issued orders to all licensed financial institutions expressly instructing the freezing of all financial assets of terrorists, terrorist organizations, individuals, and entities associated with terrorists and their organizations. Guyana has no domestic laws authorizing the freezing of terrorist assets, but the government created a special committee on the implementation of UNSCRs, co-chaired by the Head of the Presidential Secretariat and the Director General of the Ministry of Foreign Affairs. To date the procedures have not been tested, as no terrorist assets have been identified as located in Guyana. The FIU Director also disseminates the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list to relevant financial institutions.

Guyana is a member of the OAS' Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. A 2002 CICAD review of Guyana's efforts against money laundering noted numerous deficiencies in implementation, resources, and political will. Guyana is also a member of the Caribbean Financial Action Task Force (CFATF), and recently participated in CFATF's first mutual evaluation process. Guyana is a party to the 1988 UN Drug Convention. Guyana became a party to the UN Convention against Transnational Organized Crime by accession on September 14, 2004. Guyana has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

Guyana should publish regulations to implement its money laundering law and provide greater autonomy for the FIU by making it an independent unit with its own budget. Guyana should also provide appropriate resources and awareness training to its regulatory, law enforcement and prosecutorial personnel. Guyana should criminalize terrorist financing and adopt measures that would allow it to block terrorist assets.

Haiti

Haiti is not a major regional financial center, and, given Haiti's dire economic condition and unstable political situation, it is doubtful that it will become a major player in the region's formal financial sector in the near future. Money laundering and other financial crimes occur in the banking system and in casinos, foreign currency, and real estate transactions. Money laundering activity is linked to the drug trade as Haiti continues to be a major drug-transit country. While the informal economy in Haiti is significant and partly funded by narcotics proceeds, smuggling is historically prevalent and predates narcotics trafficking. Flights to Panama City, Panama, remain the main identifiable mode of transportation for money couriers. Usually travelers, predominantly Haitian citizens, hide large sums, \$30,000-\$100,000 on their persons. Haitian narcotics officers interdicting these outbound funds often collect a 6-12 percent fee and allow the couriers to continue without arrest. During interviews, couriers usually declare that they intend to use the large amounts of U.S. currency to purchase clothing and other items to be sold upon their return to Haiti, a common practice in the informal economic sector. Further complicating the picture is the cash that is routinely transported to Haiti from Haitians and their relatives in the United States in the form of remittances, representing an estimated 30 percent of Haiti's gross domestic product (GDP).

In March 2004, an interim government was established in Haiti following former President Jean Bertrand Aristide's resignation and departure. The Interim Government of Haiti (IGOH) has taken initiatives to establish improvements in economic and monetary policies as well as working to improve governance and transparency. In response to the corruption that continues to plague Haiti, the IGOH created an Anti-Corruption Unit as well as a commission to examine transactions conducted by the government from 2001 through February 2004. The commission published its report in July 2005, but to date the IGOH has not submitted for prosecution any cases based on the information provided in the report.

Despite political instability, Haiti has taken steps to address its money laundering and financial crimes problems. Since 2001, Haiti has used the Law on Money Laundering from Illicit Drug Trafficking and other Crimes and Punishable Offenses (AML Law) as its primary anti-money laundering tool. All financial institutions and natural persons are subject to the money laundering controls of the AML Law. The AML Law criminalizes money laundering and applies to a wide range of financial institutions—including banks, money changers, casinos, and real estate agents. Insurance companies are not covered; however, they are only nominally represented in the Haitian economy. The AML Law requires financial institutions to establish money laundering prevention programs and to verify the identity of customers who open accounts or conduct transactions that exceed 200,000 gourdes (approximately \$4,760). It also requires exchange brokers and transfer bureaus to obtain declarations identifying the source of funds exceeding 200,000 gourdes or its equivalent in foreign currency. The nonfinancial sector, nonetheless, remains largely unregulated.

In 2002, Haiti formed a National Committee to Fight Money Laundering, the Comité National de Lutte Contre le Blanchiment des Avoirs (CNLBA). The CNLBA is in charge of promoting, coordinating, and recommending policies to prevent, detect, and suppress the laundering of assets obtained from the illicit trafficking of drugs and other serious offenses. The financial intelligence unit (FIU) created in 2003, the Unite Centrale de Renseignements Financiers (UCREF), is responsible for receiving and analyzing reports submitted in accordance with the law. The UCREF was expanded since its creation from 8 to 42 employees, including 25 investigators. Entities are required to report to the UCREF any transaction involving funds that appear to be derived from a crime, as well as those exceeding 200,000 gourdes. Failure to report such transactions is punishable by more than three years' imprisonment. Banks are required to maintain records for at least five years and are required to present this information to judicial authorities and UCREF officials upon request. Bank secrecy or professional secrecy cannot be invoked as grounds for refusing information requests from these authorities.

The UCREF assisted in obtaining, validating and certifying Haitian bank records for use as exhibits in U.S. court proceedings. In 2005, UCREF confiscated $800,000 and froze $2.86 million related to money laundering offenses. Approximately 400 investigations were underway in 2005. Data provided largely by UCREF in 2005 resulted in the freezing of $17.6 million in assets of convicted drug trafficker Serge Edouard. The UCREF also assisted the IGOH in filing the first-ever civil lawsuit in a U.S. court for reparation of Haitian Government funds diverted through U.S. banks and businesses. Though these 2005 achievements of the UCREF are a marked improvement, the CNLBA is still not fully functional or funded, and many of the UCREF's employees still lack experience and the ability to independently investigate cases, which translates into slow progress in moving cases into the judicial system.

The AML Law has provisions for the forfeiture and seizure of assets; however the government cannot declare the asset or business forfeited until there is a conviction. The inability to seize or freeze assets early in the judicial process reduces the government's authority and resources to pursue cases. The IGOH is supportive of a stronger, more proactive asset seizure law, yet its temporary governmental mandate does not allow for the passage of new laws. The IGOH has set-up a Financial Crimes Task Force under the auspices of the Ministries of Justice, Finance, and the Central Bank, charged with identifying and investigating major financial crimes and coordinating with the UCREF in recommending prosecutions.

Supported by the U.S. Embassy Narcotics Affairs Section (NAS) and the U.S. Treasury Office of Technical Assistance (OTA), this task force and UCREF cooperated with the U.S. Internal Revenue Service in 2005 to investigate several significant cases of U.S. tax fraud. One major case developed by the task force, without U.S. assistance, is presently being prosecuted. At least six other significant cases are currently under investigation. With U.S. guidance and support, the IGOH took steps to reorganize the UCREF and the Financial Crimes Task Force. Efforts were underway at the end of 2005 to separate the intelligence gathering and investigative functions to provide for essential checks and balances and reduce the potential for internal fraud abuses.

The UCREF has three memoranda of understanding with the Dominican Republic, Panama and, Honduras. The UCREF has not yet been accepted and accredited to the Egmont Group. Haiti is a member of the OAS/CICAD Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force. Haiti is a party to the 1988 UN Drug Convention. Haiti has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Haiti still has not passed legislation specifically criminalizing the financing of terrorists and terrorism, nor has it signed the UN International Convention for the Suppression of the Financing of Terrorism. The AML Law provides for investigation and prosecution in all cases of illegally derived money. Under this law, terrorist finance assets may be frozen and seized. Currently, there is no indication of terrorist financing.

Presidential elections are scheduled for early 2006; the incoming administration should work diligently and expeditiously to fully implement and enforce the AML Law, which will require them to confront the rampant corruption present in almost all public institutions. Haiti should also further strengthen the organizational structures and personal skills of employees both in the UCREF and the

Financial Crimes Task Force. The Government of Haiti should criminalize terrorist financing and become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Honduras

Three years after passing a new law against money laundering, the Government of Honduras (GOH) has made considerable progress in implementing the law, establishing and training the entities responsible for the investigation of financial crimes, and improving cooperation among these entities. Sustained progress will depend upon increased commitment from the government to aggressively prosecute financial crimes.

Honduras is not an important regional or offshore financial center and is not considered to have a significant black market for smuggled goods, though there have been recent high-profile smuggling cases involving gasoline and other consumer goods. Money laundering takes place, primarily through the banking sector, but also through currency exchange houses and front companies. The vulnerabilities of Honduras to money laundering stem primarily from significant trafficking of narcotics, particularly cocaine, throughout the region; the smuggling of contraband may also generate funds that are laundered through the banking system. Money laundering in Honduras derives both from domestic and foreign criminal activity, and the proceeds are controlled by local drug trafficking organizations and organized crime syndicates. Honduras is not experiencing an increase in financial crimes such as bank fraud. Corruption remains a serious problem, particularly within the judiciary and law enforcement sectors.

Money laundering has been a criminal offense in Honduras since 1998, when the passage of Law No. 27-98 criminalized the laundering of narcotics-related proceeds and introduced various record keeping and reporting requirements for financial institutions. However, weaknesses in the law, including a narrow definition of money laundering, make it virtually impossible to successfully prosecute the crime.

In 2002, Honduras passed Decree No. 45-2002, which greatly strengthened its legal framework and available investigative and prosecutorial tools to fight money laundering. Under the new legislation, the definition of money laundering was expanded to include under the crime of money laundering the transfer of assets that proceed directly or indirectly from trafficking of drugs, arms, human organs or persons, auto theft, kidnapping, bank and other forms of financial fraud, and terrorism. The penalty for money laundering is a prison sentence of 15-20 years. The law also requires all persons entering or leaving Honduras to declare cash and convertible securities (títulos valores de convertibilidad inmediata) that they are carrying if the amount exceeds $10,000 or its equivalent.

Decree No. 45-2002, created the financial intelligence unit (FIU), Unidad de Informacion Financiera, within the National Banking and Securities Commission. Banks and other financial institutions are required to report to the FIU currency transactions over $10,000 in dollar denominated accounts in local currency accounts. The law requires the FIU and reporting institutions to keep a registry of reported transactions for five years. Banks are required to know the identity of all their clients and depositors, regardless of the amount of a client's deposits and to keep adequate records of the information. The law also includes banker negligence provisions that make individual bankers subject to two-to-five-year prison terms if, by "carelessness, negligence, inexperience or non-observance of the law, they permit money to be laundered through their institutions." All of the above requirements apply to all financial institutions that are regulated by the National Banking and Securities Commission, including state and private banks, savings and loan associations, bonded warehouses, stock markets, currency exchange houses, securities dealers, insurance companies, credit associations, and casinos. The law does not, however, extend to the activities of lawyers or accountants.

Decree No. 45-2002 requires that a public prosecutor be assigned to the FIU. In practice, two prosecutors are assigned to the FIU, each on a part-time basis, with responsibility for specific cases divided between them depending on their expertise. The prosecutors, under urgent conditions and with special authorization, may subpoena data and information directly from financial institutions. Public prosecutors and police investigators are permitted to use electronic surveillance techniques to investigate money laundering.

Under the Criminal Procedure Code, officials responsible for filing reports on behalf of covered entities are protected by law with respect to their cooperation with law enforcement authorities. However, some have alleged that their personal security is put at risk if the information they report leads to the prosecution of money launderers. This issue has not been present in 2005, however, as only cases originating from the police and prosecutors have been presented in court.

There had been some ambiguity in Honduran law concerning the responsibility of banks to report information to the supervisory authorities, and the duty of these institutions to keep customer information confidential. A new law passed in September 2004, the Financial Systems Law (Decree No. 129-2004), clarifies this ambiguity, explicitly stating that the provision of information requested by regulatory, judicial, or other legal authorities shall not be regarded as an improper divulgence of confidential information.

In late December 2004, Decree No. 24-2004 created the Interagency Commission for the Prevention of Money Laundering and Financing of Terrorism (CIPLAFT). The group was tasked as the coordinating entity responsible for ensuring that all anti-money laundering and anti-financing of terrorism organizations operate efficiently and consistent with all relevant laws, regulations, resolutions, and directives. The group meets every three months and includes representatives from the FIU, the Prosecutor's Office, the police and other offices that touch on the subject of money laundering and terrorist financing.

Prior to 2004, there had been no successful prosecutions of money laundering crimes in Honduras. In 2004, however, Honduran authorities arrested 16 persons for money laundering crimes, issued six additional outstanding arrest warrants, and secured five convictions. Six additional convictions were achieved in 2005.

The GOH has been supportive of counterterrorism efforts. Decree No. 45-2002 states that an asset transfer related to terrorism is a crime; however, terrorist financing has not been identified as a crime itself. This law does not explicitly grant the GOH the authority to freeze or seize terrorist assets; however, under separate authority, the National Banking and Insurance Commission has issued freeze orders for suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224.

The Ministry of Foreign Affairs is responsible for instructing the Commission to issue freeze orders. The Commission directs Honduran financial institutions to search for, hold, and report on terrorist-linked accounts and transactions, which, if found, would be frozen. The Commission has reported that to date no accounts linked to the entities or individuals on the lists have been found in the Honduran financial system.

While Honduras is a major recipient of flows of remittances (estimated at U.S. $1.5 billion in 2005), there has been no evidence to date linking these remittances to the financing of terrorism. Remittances primarily flow from Hondurans living in the United States to their relatives in Honduras. Most remittances are sent through wire transfer or bank services, with some cash probably being transported physically from the United States to Honduras. There is no significant indigenous alternative remittance system operating in Honduras, nor is there any evidence that charitable or non-profit entities in Honduras have been used as conduits for the financing of terrorism.

Under Honduran legislation, companies may register for "free trade zone" status, and benefit from the associated tax benefits, regardless of their location in the country. Companies that wish to receive free trade zone status must register within the Office of Productive Sectors within the Ministry of Industry and Commerce. The majority of companies with free trade zone status operate mostly in the textile and apparel industry. There is no indication that these free trade zone companies are being used in trade-based money laundering schemes or by the financiers of terrorism.

Honduras cooperates with U.S. investigations and requests for information pursuant to the 1988 United Nations Drug Convention. Honduras has signed memoranda of understanding to exchange information on money laundering investigations with Panama, El Salvador, Guatemala, Mexico, Peru, Colombia, and the Dominican Republic. Honduras strives to comply with the Basel Committee's "Core Principles for Effective Banking Supervision," and the new Financial System Law, Decree No. 129-2004, is designed to improve compliance with these international standards At the regional level, Honduras is a member of the Central American Council of Bank Superintendents, which meets periodically to exchange information.

Honduras is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. In November 2004, Honduras became a party to the Organization of American States (OAS) Inter-American Convention on Terrorism. Honduras is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering, and the Caribbean Financial Action Task Force (CFATF). In mid-2005, the Honduran FIU was admitted as a member in the Egmont Group.

No specific written agreement exists between the United States and Honduras to establish a mechanism for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing, and other crime investigations. However, Honduras has cooperated, when requested, with appropriate law enforcement agencies of the U.S. Government and other governments investigating financial crimes.

The Honduran Congress first enacted an asset seizure law in 1993 that subsequent Honduran Supreme Court rulings substantially weakened. Decree No. 45-2002 strengthens the asset seizure provisions of the law, establishing an Office of Seized Assets (OABI) under the Public Ministry. The law authorizes the OABI to guard and administer "all goods, products or instruments" of a crime, and states that money seized or money raised from the auctioning of seized goods should be transferred to the public entities that participated in the investigation and prosecution of the crime. Under the Criminal Procedure Code, when goods or money are seized in any criminal investigation, a criminal charge must be submitted against the suspect within 60 days of the seizure; if one is not submitted, the suspect has the right to demand the release of the seized assets.

Decree No. 45-2002 is not entirely clear on the issue of whether a legitimate business can be seized if used to launder money derived from criminal activities. The chief prosecutor for organized crime maintains that the authorities do have this power, because once a "legitimate" business is used to launder criminal assets, it ceases to be "legitimate" and is subject to seizure proceedings. However, this authority is not explicitly granted in the law, and there has been no test case to date which would set an interpretation. There are currently no new laws being considered regarding seizure of forfeiture of assets of criminal activity.

The total value of assets seized since the 2002 law came into effect is estimated at \$6.4 millions in seized assets (cars, houses, boats, etc.) as of December 2005. The lack of clear records, and differences in accounting between OABI, the Police and the Investigators Office, make prior year comparisons difficult. Most of these seized assets are alleged to have derived from crimes related to drug trafficking; none are suspected of being connected to terrorist activity. The law allows for both civil and criminal forfeiture, and there are no significant legal loopholes that allow criminals to shield their assets.

OABI has not yet established firm control over the asset seizure and forfeiture process. Implementation of the existing law, as well as the process of equipping the OABI to maintain control over seized assets and effectively dispose of them, has been slow and ineffective. The implementing regulations governing the OABI were not finalized and published until more than a year after the passage of the law, and the key regulation that governs the distribution of assets is still pending action by the Attorney General. Plans to build separate offices and a warehouse for this entity are still incomplete, resulting in seized assets currently being kept in various locations under dispersed authority. Money seized is also kept in a variety of accounts without clear records of control, or kept in cash as evidence. Due to the absence of approved implementing regulations on distribution of assets, the Public Ministry on several occasions used seized cash to pay certain employees' salaries, without the money's first having passed through a proper legal process for disposition. Similarly, assets such as vehicles, properties, and boats that are seized are in many cases are left unused, rather than being distributed for use by government agencies.

In 2005, the Government of Honduras continued its positive steps to implement Decree No. 45-2002. However, the different units involved in the fight against money laundering continue to suffer from lack of resources and limited interagency communication. Further progress in implementing the new money laundering legislation will depend on the training and retention of personnel familiar with money laundering and financial crimes and an improved ability to target and pursue more cases that have a higher probability of success. Key to enabling these agencies is to free more resources from OABI. The GOH should continue to support the developing government entities responsible for combating money laundering and other financial crimes, and ensure that resources are available to strengthen its anti-money laundering regime.

Hong Kong

Hong Kong is a major international financial center. Its low taxes and simplified tax system, sophisticated banking system, the availability of secretarial services and shell company formation agents, and the absence of currency and exchange controls, facilitate financial activity but also make it vulnerable to money laundering. The primary sources of laundered funds are narcotics trafficking (particularly heroin, methamphetamine, and ecstasy), tax evasion, fraud, illegal gambling and bookmaking, and commercial crimes. Laundering channels include Hong Kong's banking system, and its legitimate and underground remittance and money transfer networks.

Hong Kong is substantially in compliance with the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering, and has pledged to adhere to the revised FATF Forty Recommendations. Overall, Hong Kong has developed a strong anti-money laundering regime, though improvements should be made. It is a regional leader in anti-money laundering efforts. Hong Kong has been a member of the FATF since 1990.

Money laundering is a criminal offense in Hong Kong under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and the Organized and Serious Crimes Ordinance (OSCO). The money laundering offense extends to the proceeds of drug-related and other indictable crimes. Money laundering is punishable by up to 14 years' imprisonment and a fine of HK$5,000,000 (approximately $643,000).

Money laundering ordinances apply to covered institutions including banks and non-bank financial institutions, as well as to intermediaries such as lawyers and accountants. All persons must report suspicious transactions of any amount to the Joint Financial Intelligence Unit (JFIU). The JFIU does not investigate suspicious transactions itself, but receives, stores, and disseminates suspicious transactions reports (STRs) to the appropriate investigative unit. Typically, STRs are passed to either the Narcotics Bureau or the Organized Crime and Triad Bureau of the Hong Kong Police Force, or to the Customs Drug Investigation Bureau of the Hong Kong Customs and Excise Department.

Financial regulatory authorities issued anti-money laundering guidelines reflecting the revised FATF Forty Recommendations on Money Laundering to institutions under their purview, and monitor compliance through on-site inspections and other means. Hong Kong law enforcement agencies provide training and feedback on suspicious transaction reporting.

Financial institutions are required to know and record the identities of their customers and maintain records for five to seven years. The filing of a suspicious transaction report cannot be considered a breach of any restrictions on the disclosure of information imposed by contract or law. Remittance agents and money changers must register their businesses with the police and keep customer identification and transaction records for cash transactions equal to or over HK$20,000 (approximately $2,564).

Hong Kong does not require reporting of the movement of currency above any threshold level across its borders, or reporting of large currency transactions above any threshold level. However, the Narcotics Division is preparing a consultation paper regarding proposed money laundering legislation that it plans to introduce to the legislature. The proposed legislation would likely authorize Hong Kong Customs officials to stop and question passengers about money they are bringing into or taking out of Hong Kong. The draft bill would also mandate that Customs officials maintain records of individuals carrying more than $15,000 across the border, even if it is not related to a crime.

The bill would not likely mandate currency declarations at the border, but would widen the Hong Kong Government's ability to seize cash being laundered from all "serious crimes," instead of only cash stemming form narcotics trafficking or related to terrorism. Under the bill, bankers, lawyers, accountants, real estate agents, precious metals dealers, and other professionals would face criminal sanctions if they assisted in money laundering through a failure to "know their customers." The new bill would involve a statutory requirement to obtain sufficient information about the client-including the beneficial ownership of corporate clients and the source of wealth of individuals. This measure would make the failure of nonfinancial firms to report suspicious transactions an offense.

There is no distinction made in Hong Kong between onshore and offshore entities, including banks, and no differential treatment is provided for nonresidents, including on taxes, exchange controls, or disclosure of information regarding the beneficial owner of accounts or other legal entities. Hong Kong's financial regulatory regimes are applicable to residents and nonresidents alike. The Hong Kong Monetary Authority (HKMA) regulates banks. The Insurance Authority and the Securities and Futures Commission regulate insurance and securities firms, respectively. All three impose licensing requirements and screen business applicants. There are no legal casinos or Internet gambling sites in Hong Kong.

In Hong Kong, it is not uncommon to use solicitors and accountants, acting as company formation agents, to set up shell or nominee entities to conceal ownership of accounts and assets. Hong Kong registered 7,279 new international business companies (IBCs) in 2005. Many of the more than 500,000 IBCs created in Hong Kong are owned by other IBCs registered in the British Virgin Islands. Many of the IBCs are established with nominee directors. The concealment of the ownership of accounts and assets is ideal for the laundering of funds. Additionally, some banks permit the shell companies to open bank accounts based only on the vouching of the company formation agent. In such cases, the Hong Kong Monetary Authority's anti-money laundering guidelines require banks to verify the identity of the owners of the company, including beneficial owners. The bank should also assess whether the intermediary is "fit and proper". However, solicitors and accountants have filed a low number of suspicious transaction reports in recent years, and consequently have become a focus of attention to improve reporting through regulatory requirements and oversight.

The open nature of Hong Kong's financial system has long made it the primary conduit for funds being transferred out of China, which maintains a closed capital account. Hong Kong's role has been evolving as China's financial system gradually opens. On February 25, 2004, Hong Kong banks began to offer Chinese currency- (renminbi or RMB-) based, deposit, exchange, and remittance services. Later in the year, Hong Kong banks began to issue RMB-based credit cards, which could be used both in mainland China and in Hong Kong shops that had signed up to the Chinese payments system, China UnionPay. In November 2005, Hong Kong banks were permitted modest increases in the scope of RMB business they can offer to clients. The new provisions raised daily limits and expanded services. Making loans in Hong Kong in RMB, however, is still not permitted for any bank. This change brought many financial transactions related to China out of the money-transfer industry and into the more highly regulated banking industry, which is better equipped to guard against money laundering.

Under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and the Organized and Serious Crimes Ordinance (OSCO), a court may issue a restraining order against a defendant's property at or near the time criminal proceedings are instituted. Both ordinances were strengthened in January 2003, through a legislative amendment lowering the evidentiary threshold for initiating confiscation and restraint orders against persons or properties suspected of drug trafficking. Property includes money, goods, real property, and instruments of crime. A court may issue confiscation orders at the value of a defendant's proceeds from illicit activities. Cash imported into or exported from Hong Kong that is connected to narcotics trafficking may be seized, and a court may order its forfeiture.

As of September 1, 2005, the value of assets under restraint was $187 million, and the value of assets under confiscation order, but not yet paid to the government, was $14.45 million, according to figures from the JFIU. It also reported that as of September 1, 2005, the amount confiscated and paid to the government since the enactment of DTRoP and OSCO was $52.5 million, and a total of 126 persons had been convicted of money laundering over that period. Hong Kong has shared confiscated assets with the United States.

In July 2002, the legislature passed several amendments to the DTRoP and OSCO to strengthen restraint and confiscation provisions. These changes, which became effective on January 1, 2003, include the following: there is no longer a requirement of actual notice to an absconded offender; there is no longer a requirement that the court fix a period of time in which a defendant is required to pay a confiscation judgment; the court is allowed to issue a restraining order against assets upon the arrest (rather than charging) of a person; the holder of property is required to produce documents and otherwise assist the government in assessing the value of the property; and an assumption is created under the DTRoP, to be consistent with OSCO, that property held within six years of the period of the violation by a person convicted of drug money laundering is proceeds from that money laundering.

Since legislation was adopted in 1994 mandating the filing of suspicious transaction reports (STRs), the number of STRs received by JFIU has generally increased. In the first nine months of 2005, a total of 10,354 STRs were filed, compared to a total of 14,029 for the twelve months of 2004 and 11,671 for the twelve months of 2003.

A new Financial Investigations Division, established in the Narcotics Bureau, is supporting the investigations of STRs. The new division contains a section dedicated to money laundering investigations related to drug trafficking and terrorist financing. The division provides the main link with overseas and local law enforcement agencies on investigations and intelligence exchange concerning money laundering and terrorist finance. It also contains the JFIU, including a new intelligence analysis team.

The new division will analyze STRs to develop information that could aid in prosecuting money laundering cases, the number of which has also increased since 1996, soon after the passage of OSCO (1994). In terms of actual prosecutions for money laundering, there were 35 during the first 8 months of 2005, compared to 40 for the entire year of 2004 and 29 for 2003.

In July 2002, Hong Kong's legislature passed the United Nations (Anti-Terrorism Measures) Ordinance that criminalizes the supply of funds to terrorists. On July 3, 2004, the Legislative Council passed the United Nations (Anti-Terrorism Measures)(Amendment) Ordinance. This law is intended to implement UNSCR 1373 and the FATF Special Eight Recommendations on Terrorist Financing that were in place in July 2004. It extends the Hong Kong Government's freezing power beyond funds to the non-fund property of terrorists and terrorist organizations. Furthermore, it prohibits the provision or collection of funds by a person intending or knowing that the funds will be used in whole or in part to commit terrorist acts. Hong Kong's financial regulatory authorities have directed the institutions they supervise to conduct record searches for assets of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224.

The People's Republic of China represents Hong Kong on defense and foreign policy matters, including UN affairs. After the PRC becomes a party to a UN terrorism treaty, the Hong Kong Government submits implementing legislation to Hong Kong's Legislative Council. After passage, the HKG executes the relevant UN treaty. The PRC has yet to ratify the UN International Convention for the Suppression of the Financing of Terrorism.

In 2005, Hong Kong financial authorities arranged outreach activities to raise awareness of terrorism financing in the financial community. For instance, Hong Kong's bank regulatory agency, the Hong Kong Monetary Authority (HKMA), issued a circular on November 14 noting that banks were obligated to report suspicious transactions, seek legal advice on the implication of foreign laws and orders, be aware of the list of weapons of mass destruction proliferators published under U.S. Executive Order 13382, implement the latest "know your customer" principles, and ascertain the appropriateness of maintaining high-risk accounts. The HKMA circulated a guideline in June 2004 that incorporated the FATF Special Eight Recommendations on Terrorist Financing The instruction also required banks to verify fund sources before accepting money from offshore companies established with the intention of disguising beneficial ownership, correspondent banks on the FATF's non-cooperative countries and territories list, or prominent politicians and heads of state.

The rule also required banks to maintain a database of terrorist names and management information systems that detect unusual patterns of activity in customer accounts. The Securities and Futures Commission (SFC) and the Office of the Commissioner of Insurance (OCI) circulated guidance notes in 2005 that provided additional guidance on customer due diligence and other issues, reflecting the new requirements in the revised FATF Forty Recommendations on Money Laundering, and Special Recommendations on Terrorist Financing. The Hong Kong government has modified its regulations in order to make them consistent with the revised FATF Forty Recommendations on Money Laundering.

Other bodies governing segments of the financial sector are also active in anti-money laundering efforts. The Hong Kong Estates Agents Authority, for instance, has drawn up specific guidelines for real estate agents on filing suspicious transaction reports, and the Law Society of Hong Kong and the Hong Kong Institute of Certified Public Accountants are in the process of drafting such guidance.

The Hong Kong police assisted the United States in terrorism investigations in 2005. In 2003, Hong Kong took part in the International Monetary Fund's Financial Sector Assessment Program (FSAP), which aims to strengthen the financial stability of a jurisdiction by identifying the strengths and weaknesses of its financial system and assessing compliance with key international standards. As part of the FSAP, a team of IMF and World Bank-sponsored legal and financial experts assessed the effectiveness of Hong Kong's anti-money laundering regime against the FATF Forty Recommendations on Money Laundering and the FATF Special Recommendations on Terrorist Financing. The team described Hong Kong's anti-money laundering measures as "resilient, sound, and overseen by a comprehensive supervisory framework."

Through the PRC, Hong Kong is subject to the 1988 UN Drug Convention. It is an active member of the FATF and Offshore Group of Banking Supervisors and also a founding member of the Asia Pacific Group on Money Laundering (APG). Hong Kong's banking supervisory framework is in line with the requirements of the Basel Committee on Banking Supervision's "Core Principles for Effective Banking Supervision." Hong Kong's JFIU is a member of the Egmont Group and is able to share information with its international counterparts. Hong Kong is known to cooperate with foreign jurisdictions in combating money laundering.

Hong Kong's mutual legal assistance agreements generally provide for asset tracing, seizure, and sharing. Hong Kong signed and ratified a mutual legal assistance agreement with the United States that came into force in January 2000.

As of December 2005, Hong Kong had mutual legal assistance agreements with a total of 19 other jurisdictions: Australia, Canada, the United States, Italy, the Philippines, the Netherlands, Ukraine, Singapore, Portugal, Ireland, France, the United Kingdom, New Zealand, the Republic of Korea, Belgium, Switzerland, Denmark, Israel and Poland. Hong Kong has also signed surrender-of-fugitive-offenders agreements with 14 countries, and has signed Agreements for the transfer-of-sentenced-persons with seven countries, including the United States.

Hong Kong authorities exchange information on an informal basis with overseas counterparts, with Interpol, and with Hong Kong-based liaison officers of overseas law enforcement agencies. An amendment to the Banking Ordinance in 1999 allows the HKMA to disclose information to an overseas supervisory authority about individual customers, subject to conditions regarding data protection. The HKMA has entered into memoranda of understanding with overseas supervisory authorities of banks for the exchange of supervisory information and cooperation, including on-site examinations of banks operating in the host country.

The Government of Hong Kong should further strengthen its anti-money laundering regime by establishing threshold reporting requirements for currency transactions and putting into place "structuring" provisions to counter evasion efforts. Hong Kong should also establish mandatory cross-border currency reporting requirements and continue to encourage more suspicious transaction reporting by lawyers and accountants, as well as by business establishments such as auto dealerships, real estate companies, and jewelry stores. Hong Kong should also take steps to stop the use of "shell" companies, IBCs, and other mechanisms that conceal the beneficial ownership of accounts by more closely regulating corporate formation agents.

Hungary

Hungary has a pivotal location in Central Europe, with a well-developed financial services industry. Criminal organizations from Russia and other countries such as Ukraine are entrenched in Hungary. Hungarian law enforcement takes these threats seriously, forcing out a major Russian organized crime leader in 2005. The economy is largely cash-based. Money laundering is related to a variety of criminal activities, including narcotics, prostitution, and organized crime. Trafficking in humans is also a growing organized crime threat as women and children are smuggled from Russia, Romania, Ukraine, Moldova, Bulgaria, and the Balkans through Hungary en route to Scandinavian countries. Additional financial crimes such as counterfeiting of euros, real estate fraud, and the copying/stealing of bankcards are also prevalent. Financial crime has not increased in recent years, though there have been some isolated, albeit well-publicized, cases. Combating cross-border criminal activities is a priority for Hungary's law enforcement community.

Hungary became a full member of the European Union (EU) on May 1, 2004. Upon EU accession, all EU regulations became effective immediately in Hungary. As a full EU member, Hungary also is working to implement EU directives, including those relating to money laundering. Hungary had been placed on the Financial Action Task Force (FATF) list of non-cooperative countries and territories (NCCT) in the fight against money laundering in June 2001, but was removed completely from this list in the summer of 2003 due to significant improvements in its money laundering regime. Since then, it has striven to implement the FATF Forty Recommendations and the Nine Special Recommendations on Terrorist Financing.

Hungary banned offshore financial centers by Act CXII of 1996 on Credit Institutions. Offshore casinos are also prohibited from operating by the 1996 Act. There are offshore companies registered in Hungary that enjoy a preferential tax rate and are exempt from the local corporate turnover tax of two percent. Due to EU accession, however, the preferential tax treatment is being phased out and ceases at the end of 2005. Beginning in 2006, these companies are being converted automatically into Hungarian companies, subject to all Hungarian corporate taxes. The only special status they will thereafter retain is the ability to keep books in foreign currencies.

Act CXX of 2001 eliminates bearer shares and requires that all such shares be transferred to identifiable shares by the end of 2003. Thus, now all shares are subject to transparency requirements, and both owners and any beneficiaries must be registered.

By mid-2003, Hungary had successfully transferred 90 percent of anonymous savings accounts into identifiable accounts. As of December 31, 2004, such accounts can be accessed and converted only by written permission from the police.

Hungary no longer permits the operation of free trade zones. Law CXXVI of 2003 stipulates that permits for companies operating in free trade zones would expire, but allows companies to request new permits that would convert them into normal companies in 2004. The companies affected could have transferred their assets up until the end of April 2004 without a value-added tax (VAT) or customs duty. Upon Hungary's EU accession on May 1, 2004, these companies' operations immediately came under EU Council Regulation 2913/1992 and the European Commission Regulation 2454/1992. Currently, there are no companies operating in free trade zones. The Finance Ministry, however, is again planning to propose new free trade zones.

Anti-money laundering legislation in Hungary dates back to Act XXIV of 1994. Hungary's money laundering legislation covers all serious crimes punishable by imprisonment. In 2003, the Government of Hungary (GOH) re-codified its money laundering legislation in Act XV of 2003, "On the Prevention and Impeding of Money Laundering," which became effective on June 16, 2003. The 2003 Act extends the anti-money laundering legislation to encompass the following additional professions and business sectors: financial services, investment services, insurance, stock brokers, postal money transfers, real estate agents, auditors, accountants, tax advisors, gambling casinos, traders of gems or other precious metals, private voluntary pension funds, lawyers, and public notaries. Act XV also criminalizes tipping off and forces self-regulating professions to submit internal rules to identify asset holders, track transactions, and report suspicious transactions. In April 2002, Section 303 of the Penal Code on Money Laundering was amended to criminalize as punishable offenses the laundering of one's own proceeds, laundering through negligence, and conspiracy to commit money laundering.

Hungary's financial regulatory body, the Hungarian Financial Supervisory Authority (HFSA), is charged with supervising all types of financial service providers. The one exception to this is cash processing, which is supervised by Hungary's Central Bank, the National Bank of Hungary. Auditors, casinos, lawyers, and notaries are supervised by their own trade associations. The Hungarian National Police (HNP) supervises all other professions covered under the 2003 Act, because they have neither self-regulatory professional bodies nor state supervision.

The 2003 Act also states that if an individual carries currency exceeding one million HUF (approximately $5,300) across a border, the amount must be declared in writing to the customs authority. Customs authorities are also obligated to establish the identity of an individual crossing the border if any suspicion of money laundering arises.

As of 2001, only banks or their authorized agents can operate currency exchange booths. These exchange booths are subject to “double supervision,” as they are subject to the banks’ internal control mechanisms, which are in turn subject to supervision by the HFSA. The exchange booths are required to verify customer identity for currency exchange transactions totaling or exceeding HUF 300,000 (approximately $1,600). These amounts can come either from a single transaction or consecutive separate transactions exceeding this threshold. The exchange booths are also required to file suspicious transaction reports for currency exchange transactions in any amount. There are currently about 300 exchange booths in Hungary.

The 2003 Act also states that covered service providers are required to identify their customers or any authorized individual representing their customers, when entering into a business relationship. In transactions exceeding two million HUF (approximately $10,600) or transactions of any amount where suspicion of money laundering arises, the customer must be identified. Under the anti-money laundering legislation, banks, financial institutions, and other service providers are required to maintain records for at least ten years. All service providers are required to report suspicious transactions directly, or through their representation bodies, to the police authority as soon as they occur. Lawyers and notaries are exempt from their reporting obligations only when they are representing their clients in a criminal court case. Under all other circumstances, they are obligated to file reports. Both lawyers and notaries submit their reports to their respective bar and notary associations, which then forward the reports on to the police. All other service providers submit their reports directly to the police. The police may perform on-site random checks of service providers. According to Hungarian bank secrecy regulations, financial service providers are obliged to supply law enforcement authorities with relevant data.

When these professions were included in the anti-money laundering legislation of 2003, there were some initial concerns and protests as to how the legislation would be put into practice. As the police briefed representatives of these professions and rules were adopted, the concerns have diminished. Currently, only antique shops are known still to have concerns, although they are believed to be meeting their reporting obligations.

Reporting individuals are protected in their anti-money laundering reporting obligations. If the report involves suspicious activity related to terrorist financing, the law allows for the possibility of protection. Currently, however, actual extension of protection is granted at the discretion of the prosecutor.

Hungary’s financial intelligence unit (FIU) is part of the HNP. It investigates money laundering cases and has considerable authority to request and release information, nationally and internationally. In the summer of 2004, the HNP completed a major organizational restructuring that included the establishment of the National Bureau of Investigation (NBI). Among its mandates, the NBI is charged with the detection and investigation of major corruption and money laundering cases. One of the main objectives of this restructuring was to eliminate the parallel jurisdictions that existed between the Financial Crime Investigation and Economic Crime Investigation areas and to implement a more coordinated investigative effort for money laundering investigations. The combined Economic and Financial Crimes Department of the NBI has a staff of 134 at the headquarters level. The FIU within this department has a staff of 42. In 2004, it received 14,120 STRs. Reportedly, the number of STRs received in 2005 was expected to remain similar to that of 2004. An increase in the number of investigators has helped the FIU investigate cases.

In 2003, a money laundering scandal surfaced involving a Hungarian subsidiary, K&H Equities, of a Dutch-owned bank. A broker reportedly skimmed funds from some clients in order to pad the returns of other more favored clients. Money was laundered through several banks. The case is currently before the courts. After it was discovered that bank tellers had failed to file STRs in the K&H case, "banker negligence" laws were enacted that made individual bankers responsible if their institutions launder money. According to the Hungarian FIU, this has resulted in over-reporting.

The Hungarian Criminal Code, Act XIX of 1998, and amended by Act II of 2003, contains a provision on the forfeiture of assets. Under this provision, assets that were used to commit crimes, would endanger public safety, or were created as a result of criminal activity, are subject to forfeiture. All property related to criminal activity during the period of time when the owner was a party to a criminal organization can be seized, unless proven to have been obtained in good faith as due compensation. Act II of 2003 states that persons or members of criminal organizations sponsoring activities of a terrorist group by providing material assets or any other support face five to fifteen years of imprisonment.

The Hungarian Criminal Code treats terrorist financing-related crimes differently than all other crimes. For all other crimes, the police freeze the assets and must then inform the bank within 24 hours as to whether there will be an investigation. Police investigations must be completed within two years of filing charges. Forfeiture and seizure for all crimes, including terrorist financing, is determined by a court ruling. The banking community has cooperated fully with enforcement efforts to trace funds and seize/freeze bank accounts. In all cases, some of the frozen assets may be released, for example, to cover health-related expenses or basic sustenance, if the FIU approves a written request from the owner of the assets. After subtracting any related civil damages, proceeds from asset seizures and forfeitures go to the government.

Act IV of 1978, Article 261, criminalizes terrorist acts. Hungary criminalizes terrorism and all forms of the financing of terrorism by Act II of 2003, which modifies Criminal Code Article 261. This includes providing funds or collecting funds for terrorist actions or facilitating or supporting such actions by any means. The penalty for such crimes is imprisonment of five to fifteen years.

Hungary can also freeze terrorist finance-related assets. Act XIX of 1998 on Criminal Procedures, Articles 151, 159, and 160, provide for the immediate seizure, sequestration, and precautionary measures against terrorist assets. In cases where terrorist financing is suspected, banks freeze the assets and then promptly notify HFSA, the FIU, and the Ministry of Finance. The FIU must inform the banks within 24 hours whether or not it will conduct an investigation. The GOH circulates to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. In 2003, there was one arrest for terrorist financing, when a foreigner attempted to donate to a charitable organization listed on the UN's consolidated list of terrorists. The bank immediately froze the assets, but the individual was deported from the country without the case going to trial. In 2004, there was one suspected case of terrorist financing. Assets were frozen in a bank account that received a transfer from a bank in Saudi Arabia. However, the court ruled that the recipient of the funds could not be judged guilty solely on the basis of receiving funds from an entity on the UN's consolidated list of suspected terrorists.

Act CXII of 1996 on Credit Institutions bans the use of any indigenous alternative remittance systems that bypass, in whole or in part, financial institutions. In cases where money is transferred to a charitable or non-profit entity, the GOH has proven it will freeze the assets regardless of the amount, as was true in the one notable case in 2003.

Hungary and the United States have a Mutual Legal Assistance Treaty and a non-binding information-sharing arrangement with the United States that is intended to enable U.S. and Hungarian law enforcement to work more closely to fight organized crime and illicit transnational activities. In furtherance of this goal, in May 2000, Hungary and the U.S. Federal Bureau of Investigation established a joint task force to combat Russian organized crime groups. Hungary has signed bilateral agreements with 41 other countries to cooperate in combating terrorism, drug-trafficking, and organized crime.

Hungary is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and underwent a third round mutual evaluation in 2005. Hungary's FIU has been a member of the Egmont Group since 1998.

In 2000, Hungary signed and ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Hungary is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. The GOH signed the UN Convention against Corruption on December 10, 2003 and ratified it on April 19, 2005.

Hungary has made progress in developing its anti-money laundering regime. However, continued effort is needed with regard to implementation. Also, an increased level of cooperation and coordination is needed among the different law enforcement entities involved in the anti-money laundering regime in Hungary. Additional training for prosecutors, judges, and police is also necessary in order to promote the successful prosecution of money laundering cases. Increased AML/CFT training for employees of financial institutions and other obliged entities is also necessary in order to effectively combat the rise in defensive reporting.

India

India's status as a growing regional financial center, its large system of informal cross-border money flows and its widely perceived tax avoidance problem all contribute to the country's vulnerability to money laundering activities. Some common sources of illegal proceeds in India are narcotics trafficking, trade in illegal gems (particularly diamonds), smuggling, trafficking in persons, corruption, and income tax evasion. India is a major drug-transit country.

India's historically strict foreign-exchange laws and transaction reporting requirements, together with the banking industry's "know-your-customer" policy, make it difficult for criminals to use banks or other financial institutions to launder money. Large portions of illegal proceeds are accordingly laundered through the alternative remittance system called "hawala" or "hundi." The hawala market is estimated at anywhere between 30 and 40 percent of the formal market. Remittances to India reported through legal, formal channels in 2004-2005 amounted to $20.5 billion.

Under the hawala system, individuals transfer value from one location to another, often without the actual movement of currency. Key features of the hawala system are that it transfers value without actually moving funds. When accounts need to be balanced between hawaladars, a number of techniques are used including cash and bank transfers. But historically and culturally, trade is the most common vehicle to provide "counter valuation." This is often accomplished through invoice manipulation such as over and under valuation. Any commodity can be used in hawala value transfer but gold remains most popular. The hawala system provides anonymity and security to transacting individuals. Reportedly, many Indians do not trust banks and prefer to avoid the lengthy paperwork required to complete a money transfer through a financial institution. Hawala dealers can provide the same remittance service as a bank with little or no documentation and at rates less than those charged by banks. The Government of India (GOI) neither regulates hawala dealers nor requires them to register with the government. The Reserve Bank of India (RBI), the country's Central Bank, argues that the widespread hawala dealers operate illegally and therefore cannot be registered and are beyond the reach of regulation. Reportedly, the RBI does intend to increase its regulation of non-bank money transfer operations by entities such as currency exchange kiosks and wire transfer services.

Historically, gold has been one of the most important commodities involved in Indian hawala transactions. There is a widespread cultural demand for gold in the region. (India liberalized its gold trade restrictions in the mid-1990s). In recent years, it is thought that the growing Indian diamond trade has also been increasingly important in providing countervaluation, a method of "balancing the books" in external hawala transactions. Invoice manipulation (for example, inaccurately reflecting the value of a good sold on the invoice) is pervasive and is used extensively to both avoid customs duties and taxes and to launder illicit proceeds through trade-based money laundering.

India has both legal and illegal unregulated black market channels for selling goods. Smuggled goods such as food items, computer parts, cellular phones, gold, and a wide range of imported consumer goods are routinely sold through the black market. By avoiding customs duties and taxes and dealing in cash transactions, black market merchants offer better prices than those offered by regulated merchants. However, with trade liberalization and the increase in the number of foreign companies doing business in India, the volume of business in smuggled goods has fallen significantly. Most products previously sold through the black market are now sold through lawful channels.

Tax evasion is also widespread. Changes in the tax system are gradually being implemented, as the GOI now requires individuals to use a personal identification number to pay taxes, purchase foreign exchange, and apply for passports. The GOI introduced a value added tax (VAT) in April 2005. This tax replaces a basket of complicated state sales taxes and excise taxes, thus reducing the incentive and opportunities for businesses to conceal their sales or income levels. Twenty-one Indian states have already implemented the VAT, and the GOI anticipates that the remaining nine states will do so by April 2006.

The Criminal Law Amendment Ordinance allows for the attachment and forfeiture of money or property obtained through bribery, criminal breach of trust, corruption, or theft, and of assets that are disproportionately large in comparison to an individual's known sources of income. The 1973 Code of Criminal Procedure, Chapter XXXIV (Sections 451-459), establishes India's basic framework for confiscating illegal proceeds. The Narcotic Drugs and Psychotropic Substances Act (NDPSA) of 1985, as amended in 2000, calls for the tracing and forfeiture of assets that have been acquired through narcotics trafficking, and prohibits attempts to transfer and conceal those assets. The Smugglers and Foreign Exchange Manipulators Act (SAFEMA) also allows the seizure and forfeiture of assets linked to Customs Act violations. The competent authority (CA), located in the Ministry of Finance (MOF), administers both the NDPSA and SAFEMA.

Amendments to the NDPSA dating from 2001 allow the CA to seize any asset owned or used by a narcotics trafficker immediately upon arrest; previously, assets could be seized only after conviction. However, Indian law enforcement officers lack training in the procedures for identifying individuals who might be subject to asset seizure/forfeiture, and in tracing assets to be seized. They also appear to lack sufficient training in drafting and expeditiously implementing asset freezing orders. During 2005, the CA held nine asset seizure and forfeiture workshops pursuant to the NDPSA in New Delhi, Himchal Pradesh, Uttar Pradesh, Rajasthan, and Andra Pradesh, to train law enforcement officers in asset seizure and forfeiture procedures and regulations. The GOI hopes the training will lead to increased seizures and forfeitures from illicit narcotics proceeds.

The Foreign Exchange Management Act (FEMA), which was enacted in 2000, is one of the GOI's primary tools for fighting money laundering. The FEMA's objectives include the establishment of controls over foreign exchange, the prevention of capital flight, and the maintenance of external solvency. FEMA also imposes fines on unlicensed foreign exchange dealers. A closely related piece of legislation is the Conservation of Foreign Exchange and Prevention of Smuggling Act (COFEPOSA), which provides for preventive detention in smuggling and other matters relating to foreign exchange violations. The MOF's Directorate of Enforcement (DOE) enforces FEMA and COFEPOSA. The RBI also plays an active role in the regulation and supervision of foreign exchange transactions.

On November 27, 2002, the lower house of Parliament finally passed the Prevention of Money Laundering Act (PMLA), which had first been introduced in 1998. The bill was amended in August

2002 by the upper house to include terrorist financing provisions. India's President signed the law in January 2003. This legislation criminalizes money laundering, establishes fines and sentences for money laundering offenses, imposes reporting and record keeping requirements on financial institutions, provides for the seizure and confiscation of criminal proceeds, and provides for the creation of a Financial Intelligence Unit (FIU). Implementing rules and regulations for the PMLA were promulgated in July 2005. Penalties for offenses under the PMLA are severe and may include imprisonment for three to seven years and fines as high as $10,280. If the money laundering offense is related to a drug offense under the NDPSA, imprisonment can be extended to a maximum of ten years. The PMLA mandates that banks, financial institutions and intermediaries (including stock market intermediaries such as brokers) maintain records of all cash transactions exceeding $21,740. However, there have been no prosecutions or convictions under the PMLA since its inception.

With the notification of the PMLA in July 2005, India is establishing a central financial intelligence unit (FIU) to centralize and coordinate most of its anti-money laundering and counter terrorist financing strategies. The FIU will be an independent unit located within the Central Economic Intelligence Bureau (CEIB), under the administrative control of the MOF's Department of Revenue. The MOF has authorized 43 positions for the FIU, including a director (joint secretary), seven additional directors, one technical director, ten technical officers, and clerical personnel. This multi-disciplinary team of officers will be seconded for a two-year rotation. The directors are from various government agencies—Police, Revenue Department, Income Tax, Customs, RBI, Intelligence Bureau, Securities and Exchange Board of India (SEBI), and the Legal Affairs Department of the Ministry of Law. The FIU expects to have all these positions filled, and to begin receiving suspicious transaction reports (STRs) by March 2006.

The FIU will be solely responsible for receiving, processing, analyzing, and disseminating information on STRs, and will independently refer suspicious cases to the appropriate enforcement agency. The MOF's Enforcement Directorate will handle the investigations and prosecution of money laundering cases. The GOI has established an Economic Intelligence Council (EIC) to enhance coordination among the various enforcement agencies and directorates in the MOF. The EIC provides a forum for enforcement agencies to strengthen intelligence and operational coordination, to formulate common strategies to combat economic offenses, and to discuss cases requiring interagency cooperation. In addition to the EIC, there are 18 regional economic committees in India. The CEIB will function as the secretariat for the EIC. The CEIB interacts with the National Security Council, the Intelligence Bureau, and the Ministry of Home Affairs on matters concerning national security and terrorism.

The FIU's core team will phase in its operations as follows: Phase 1, beginning in January 2006, will entail the bulk filing of information manually and the securing of this information electronically on CDs. Phase two, with a target date of June 2006, will focus on firming up formats and analytical tools, customization of requirements, and testing of analytical tools. The final phase, to be completed by December 2006, will include the sharing of information domestically and with other FIUs, the latter on a case-by-case basis. The FIU and the MOF are making all efforts to become compliant with Egmont standards with the ultimate goal of becoming a member of the Egmont Group.

The Central Bureau of Investigation, the Directorate of Revenue Intelligence, Customs, and Excise, the RBI, the Competent Authority, and the MOF are all active in anti-money laundering efforts. In 2004, the Directorate of Revenue Intelligence (DRI) referred four hawala-based money laundering cases with a U.S. nexus to the U.S. Department of Homeland Security/Immigration and Customs Enforcement (DHA/ICE). DHS/ICE carried out successful investigations on three of these cases and forwarded tangible results to the MOF's DOE. In 2005, the DOE forwarded two additional hawala-linked money laundering cases to DHS/ICE. DHS/ICE has provided investigative assistance.

Many banking institutions, prompted by the RBI, have taken steps on their own to combat money laundering. Many banks have compliance officers to ensure that anti-money laundering regulations are observed. The RBI issued a notice in 2002 to commercial banks instructing them to adopt the "know-your-customer rules". The Indian Bankers Association established a working group to develop self-regulatory anti-money laundering procedures. Foreign customers applying for accounts in India must show positive proof of identity when opening a bank account. Banks also require that the source of funds must be declared if the deposit is more than the equivalent of $10,000. Finally, banks must report suspicious transactions. The GOI has the power to order banks to freeze assets. In November 2004, the RBI issued a circular updating its know-your-customer guidelines drafted to ensure that they comply with Financial Action Task Force (FATF) recommendations. The guidelines include the requirement that banks identify politically connected account holders residing outside India and identify the source of funds before accepting deposits from these individuals. The RBI has placed politically exposed persons (those entrusted with prominent public functions in other countries) in the highest risk category for the commission of financial crimes. The RBI also asked all commercial banks to become FATF-compliant regarding customer identification for existing as well as new accounts by December 2005.

India does not have an offshore financial center but does license offshore banking units (OBUs). These OBUs are required to be predominantly owned by individuals of Indian nationality or origin resident outside India and include overseas companies, partnership firms, societies and other corporate bodies. OBUs must also be audited to affirm that ownership by a nonresident Indian is not less than 60 percent. These entities are susceptible to money laundering activities, in part because of a lack of stringent monitoring of transactions in which they are involved. Finally, OBUs must be audited financially, but the firm that does the auditing does not have to have government approval.

India is a party to the 1988 UN Drug Convention, and is a member of the Asia/Pacific Group on Money Laundering. It is a signatory to, but has not yet ratified, the UN Convention against Transnational Organized Crime. India is a party to the UN International Convention for the Suppression of the Financing of Terrorism. In October 2001, the GOI and the United States signed a mutual legal assistance treaty, which entered into force in October 2005. India has also signed a police and security cooperation protocol with Turkey, which among other things provides for joint efforts to combat money laundering The GOI is implementing this convention through the Unlawful Activities Prevention Act. India is a party to 1988 UN Drug (Vienna) Convention. India implements the 1988 UN Drug Convention through amendments to the NDPSA (in 1989 and 2001) and the PMLA. It signed the Palermo Convention in December 2002 but has not yet ratified it.

India is a member of INTERPOL, and the CBI is the official INTERPOL unit in India. All state police forces and other law enforcement agencies have a link through INTERPOL/New Delhi to their counterparts in other countries for purposes of criminal investigations. India's Customs service is a member of the World Customs Organization, and shares enforcement information with countries in the Asia/Pacific region.

The GOI maintains tight controls over charities, which are required to register with the RBI. In April 2002, the Indian Parliament passed the Prevention of Terrorism Act (POTA), which criminalizes terrorist financing. In March 2003, the GOI announced that it had charged 32 terrorist groups under the POTA and had notified three others that they were involved in what were considered illegal activities. In July 2003, the GOI announced that it had arrested 702 persons under the POTA. In November 2004, the Parliament repealed the POTA and amended the 1967 Unlawful Activities (Prevention) Act to include the POTA's salient elements, including the criminalization of terrorist financing and the legal definitions for terrorism and terrorist acts. A GOI/POTA review committee will have one year review all 333 pending POTA cases, after which time any case that is not resolved will be dismissed. Terrorist financing in India, as well as in much of the subcontinent, is linked to the hawala system. The Government of India should cooperate fully with international initiatives to provide increased transparency in hawala, and, if necessary should initiate regulation and increase law enforcement actions in this area. Indian citizens' involvement in the underworld of the international diamond trade should be examined. It also needs to quickly finalize the implementing regulations to the anti-money laundering law and ensure that the new FIU is fully operational in order to disseminate suspicious transaction reports to domestic law endowment and enhance information sharing with other FIUs globally. Meaningful tax reform will also assist in negating the popularity of hawala and lessen money laundering. Increased enforcement action should also be taken to combat trade-based money laundering. India should become a party to the UN Convention against Transnational Organized Crime.

Indonesia

Although neither a regional financial center nor an offshore financial haven, Indonesia is vulnerable to money laundering and terrorist financing due to a poorly regulated financial system, the lack of effective law enforcement and widespread corruption. Most money laundering in the country is connected to non-drug criminal activity such as gambling, prostitution, bank fraud, piracy and counterfeiting, illegal logging and corruption. Indonesia also has a long history of smuggling, facilitated by thousands of miles of un-patrolled coastline and a law enforcement system riddled with corruption. The proceeds of these illicit activities are easily parked offshore and only repatriated as required for commercial and personal needs.

As a result of Indonesia's ongoing efforts to implement the reforms to its Anti-Money Laundering (AML) regime, the Financial Action Task Force (FATF) removed Indonesia from its list of Non-Cooperative Countries and Territories (NCCT) on February 11, 2005. In order to ensure continued effective implementation of the reforms enacted, the FATF is monitoring Indonesia's progress for one year. The removal of Indonesia from the NCCT list recognized a concerted, interagency effort—personally directed by President Susilo Bambang Yudhoyono—to further develop Indonesia's nascent AML regime.

Indonesia's Financial Intelligent Unit (PPATK), established in December 2002 and fully functional since October 2003, continues to make steady progress in developing its human and institutional capacity. The PPATK is an independent agency that receives, maintains, analyzes, and evaluates currency and suspicious financial transactions, provides advice and assistance to relevant authorities, and issues publications. As of December 16, the PPATK has received approximately 3,059 suspicious transactions reports (STRs) from 102 banks and 23 non-bank financial institutions. The volume of STRs has increased from an average of 70 per month in 2004, to 160 per month in 2005. The agency also reported that it had received over 1.4 million cash transaction reports (CTRs). Based on their analysis of 646 STRs, PPATK investigators have referred 344 cases to the police. Based on referrals of STRs and other related information from the PPATK, as of September 2005, there has been 1 successful prosecution involving terrorism, 19 successful prosecutions involving bank fraud and/or corruption, and 1 successful prosecution for money laundering. Sentences in these cases ranged from 4 months in prison to the death penalty. Fifteen of the twenty one cases had sentences imposed of 8 years in prison or more; the money laundering verdict handed down a sentence of 8 years in prison.

Indonesia's Anti-Money Laundering and Counter Terrorism Finance (CTF) Donors' Coordination Group, co-chaired by the PPATK and the Australian Agency for International Development (AUSAID), has become a model for AML/CTF donors' coordination groups in other countries. Since Indonesia's removal form the NCCT list, donors and the Government of Indonesia (GOI) have placed greater emphasis on more practical training; technical and capacity building assistance for the non-bank financial sector, police, prosecutors and judges; cash smuggling; and regulation of charities and money changers.

The PPATK is actively pursuing broader cooperation with relevant GOI agencies. The PPATK has signed nine domestic memoranda of understanding (MOUs) to assist in financial intelligence information exchange with the following entities: Attorney General's Office (AGO) Bank Indonesia

(BI), the Capital Market Supervisory Agency (Bapepam), the Directorate General of Financial Institutions, the Directorate General of Taxation, Director General for Customs and Excise the Center for International Forestry Research, the Indonesian National Police, the Ministry of Forestry and the Corruption Eradication Committee.

Sustained public awareness campaigns, new bank and financial institution disclosure requirements, and the PPATK's support for Indonesia's first credible anticorruption drive have led to increased public awareness about money-laundering and, to a lesser degree, terrorism finance. Weak human and technical capacity, poor interagency cooperation, and corruption, however, still remain significant impediments to the continuing development of an effective and credible AML regime.

Until recently, banks and other financial institutions did not routinely question the sources of funds or require identification of depositors or beneficial owners. Financial reporting requirements were put in place only in the wake of the 1998 Asian financial crisis when the GOI became interested in controlling capital flight and recovering foreign assets of large-scale corporate debtors or alleged corrupt officials.

In April 2002, Indonesia passed Law No. 15/2002 Concerning the Crime of Money Laundering, Indonesia's anti-money laundering (AML) law, which made money laundering a criminal offense. The law identifies 15 predicate offenses related to money laundering, including narcotics trafficking and most major crimes. Law No. 15/2002 established the PPATK to develop policy and regulations to combat money laundering and terrorist finance.

In September 2003, Parliament passed Law No. 25/2003 amending Law No. 15/2002 Concerning the Crime of Money Laundering that addressed many FATF concerns. Amending Law No. 25/2003 provides a new definition of the crime of money laundering making it an offense for anyone to deal intentionally with assets known or reasonably suspected to constitute proceeds of crime with the purpose of disguising or concealing the origins of the assets, as seen in Articles 1(1) and 3. The amendment removes the threshold requirement for proceeds of crime and expands the definition of proceeds of crime to cover assets employed in terrorist activities. Article 1(7)(c) expands the scope of regulations requiring STRs to include attempted or unfinished transactions. Article 13(2) shortens the time to file an STR to three days or less after the discovery of an indication of a suspicious transaction. Article 17A makes it an offense to disclose information about the reported transactions to third parties, which carries a maximum of five years' imprisonment and a maximum of one billion rupiah (approximately $100,000). Articles 44 and 44A provide for mutual legal assistance with respect to money laundering cases, with the ability to provide assistance using the compulsory powers of the court. Article 44B imposes a mandatory obligation on the PPATK to implement provisions of international conventions or international recommendations on the prevention and eradication of money laundering. The Ministry of Justice and Human Rights finalized a draft Mutual Legal Assistance Law in early 2005 and the draft was sent from the President to the Parliament on June 9, 2005, for approval. Until this legislation is formally passed, the GOI uses informal, non-binding procedures to facilitate MLA from other states.

Bank Indonesia (BI), the Indonesian Central Bank, issued Regulation No. 3/10/PBI/2001, "The Application of Know Your Customer Principles," on June 18, 2001. This regulation requires banks to obtain information on prospective customers, including third party beneficial owners, and to verify the identity of all owners, with personal interviews if necessary. The regulation also requires banks to establish special monitoring units and appoint compliance officers responsible for implementation of the new rules and to maintain adequate information systems to comply with the law. Finally, the regulation requires banks to analyze and monitor customer transactions and report to BI within seven days any "suspicious transactions" in excess of Rp 100 million (approximately $10,000). The regulation defines suspicious transactions according to a 39-point matrix that includes key indicators such as unusual cash transactions, unusual ownership patterns, or unexplained changes in transactional behavior. BI specifically requires banks to treat as suspicious any transactions to or from countries "connected with the production, processing and/or market for drugs or terrorism."

BI has issued an Internal Circular Letter No. 6/50/INTERN, dated September 10, 2004 concerning Guidelines for the Supervision and Examination of the Implementation of KYC and AML by Commercial Banks. In addition, BI also issued a Circular Letter to Commercial Banks No. 6/37/DPNP dated September 10, 2004 concerning the Assessment and Imposition of Sanction on the Implementation of KYC and other Obligation Related to Law on Money Laundering Crime. BI is also preparing Guidelines for Money Changers on Record Keeping and Reporting Procedures and Money Changer Examinations given by BI examiners.

Currently, banks must report all foreign exchange transactions and foreign obligations to BI. With respect to the physical movement of currency, Article 16 of Law No. 15/2002 contains a reporting requirement for any person taking cash into or out of Indonesia in the amount of 100 million Rupiah (approximately $10,000) or more, or the equivalent in another currency, which must be reported to the Director General of Customs. These reports must be given to the PPATK in no later than five business days and contain details of the identity of the person. Indonesian Central Bank regulation 3/18/PBI/2001 and the Directorate General of Customs and Excise Decree No.01/BC/2005 contain the requirements and procedures of inspection, prohibition, deposit of Indonesia Rupiah into or out of Indonesia. The Decree provides implementing guidance for Ministry of Finance Regulation No.624/PMK.04/2004 of December 31, 2004, which requires individuals who import or export more than rupiah 50 to 100 million in cash (approximately $5,000-$10,000) to report such transactions to Customs. This information is to be declared on the Indonesian Customs Declaration (BC2.2) and Customs officials at Jakarta, Batam and Pekanbaru airports submitted 325 such forms between January 19 and August 31, 2005, with 200 submitted after May 2.

Indonesia's bank secrecy law covers information on bank depositors and their accounts. Such information is generally kept confidential and can only be accessed by the authorities in limited circumstances. However, Article 27(4) of the Law No. 15/2002 now expressly exempts the PPATK from "the provisions of other laws related to bank secrecy and the secrecy of other financial transactions" in relation to its functions in receiving and requesting reports and conducting audits of providers of financial services. In addition, Article 14 of the Law No. 15/2002 exempts providers of financial services from bank secrecy provisions when carrying out their reporting obligations, and Article 15 of their anti-money laundering legislation gives providers of financial services, their officials and employees protection from civil or criminal action in making such disclosures.

Indonesia's laws provide only limited authority to block or seize assets. Under BI regulations 2/19/PBI/2000, police, prosecutors, or judges may order the seizure of assets of individuals or entities that have been either declared suspects, or indicted for a crime. This does not require the permission of BI, but, in practice, for law enforcement agencies to identify such assets held in Indonesian banks, BI's permission would be required. In the case of money laundering as the suspected crime, however, bank secrecy laws would not apply, according to the anti-money laundering law.

The GOI does have the authority to trace and freeze assets of individuals or entities on the UNSCR 1267 Sanctions Committee's consolidated list, and through BI, has circulated the consolidated list to all banks operating in Indonesia, with instructions to freeze any such accounts. The interagency process to issue freeze orders, which includes the Foreign Ministry, Attorney General, Police, and BI, takes several weeks from UN designation to bank notification. The implementation of this process has not led to the discovery of accounts or assets of individuals or entities on UN 1267 consolidated list. However, during the course of terrorism investigations, the Indonesia police have located and frozen accounts of individuals on the UN 1267 consolidated list.

The GOI is currently drafting additional amendments to Law No. 15/2002 that would provide the PPATK with preliminary investigative authority and the ability to temporarily freeze assets. The amendments are intended to provide technical investigative support to police and prosecutors and to deter capital flight. Indonesia's AML Law and Government Implementing Regulation No. 57/2003 provide protections to whistleblowers and witnesses. The GOI has also finalized a whistleblower and witness protection law, which is now under parliamentary consideration.

The October 18, 2002, emergency counterterrorism regulation, the Government Regulation in Lieu of Law of the Republic of Indonesia (Perpu), No. 1 of 2002 on Eradication of Terrorism criminalizes terrorism and provides the legal basis for the GOI to act against terrorists, including the tracking and freezing of assets. The Perpu provides a minimum of three years and a maximum of 15 years imprisonment for anyone who is convicted of intentionally providing or collecting funds that are knowingly used in part or in whole for acts of terrorism. This regulation is necessary because Indonesia's anti-money laundering law criminalizes the laundering of "proceeds" of crimes, but it is often unclear to what extent terrorism generates proceeds. In October 2004, an Indonesian court convicted and sentenced one Indonesian to four years in prison on terrorism charges connected to his role in the financing of the August 2003 bombing of the Jakarta Marriott Hotel.

The GOI has just begun to take into account alternative remittance systems or charitable or nonprofit entities in its strategy to combat terrorist finance and money laundering. The PPATK has issued guidelines for non-bank financial service providers and money remittance agents on the prevention and eradication of money laundering and the identification and reporting of suspicious and other cash transactions. The GOI recently initiated a dialogue with charities and nonprofit entities on improving regulation and oversight of those sectors.

Indonesia is an active member of the Asia/Pacific Group on Money Laundering (APG) and the Bank for International Settlements. BI claims that it voluntarily follows the Basel Committee's "Core Principles for Effective Banking Supervision." The GOI is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Indonesia has signed, but not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

In June 2004, Indonesia became a member of the Egmont Group and, as such, is bound to share financial intelligence with other members in accordance with the organization's charter. The PPATK is actively pursuing broader cooperation with other Financial Intelligence Units (FIUS) and has MOUs with Thailand, Malaysia, Republic of Korea, Philippines, Romania, Australia, Belgium, Italy, Spain, Poland and Peru. The PPATK has also entered into an Exchange of Letters enabling international exchange with Hong Kong. Indonesia has signed Mutual Legal Assistance Treaties with Australia, China and South Korea, and Indonesia joined other ASEAN nations in signing the ASEAN Treaty on Mutual Legal Assistant in Criminal Matter on November 29, 2004. The Indonesian Regional Law Enforcement Cooperation Centre was formally opened in 2005 and was created to develop the operational law enforcement capacity needed to fight transnational crimes.

The GOI should continue its steady progress in strengthening its anti-money laundering regime to make it more effective. In particular, it must improve interagency cooperation in investigating and prosecuting cases. In this regard, Indonesia should review the adequacy of its Code for Criminal Procedure and Rules of Evidence and enact legislation to allow the use of modern techniques to enter evidence in court proceedings. Indonesia should also enact mutual legal assistance legislation as soon as possible and cooperate closely with other countries in providing and receiving this assistance. Indonesia should review and streamline its process for reviewing UN designations and identifying, freezing and seizing terrorist assets. Indonesia should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and should ratify the UN Convention against Transnational Organized Crime.

Iran

The U.S. Department of State has designated Iran as a State Sponsor of Terrorism. No new information has been reported for Iran in 2005, so this report repeats information from last year and may be therefore be outdated in some aspects.

Iran is not a regional financial center. Iran has a robust underground economy and the use of alternative remittance systems like hawala to launder money is widespread. The underground economy is spurred—in part—by attempts to avoid restrictive taxation. In 2003, a prominent Iranian banking official was quoted as estimating that money laundering encompasses 20 percent of Iran's economy and that the under-development of financial institutions leads to an imbalance in financial markets causing underground financial activities to flourish. Further, Iran's real estate market is used to launder money. Real estate transactions take place in Iran, but often no funds change hands there; rather, payment is made overseas. This is typically done because of the difficulty in transferring funds out of Iran and the weakness of Iran's currency, the rial.

Hawala is also used to transfer value to and from Iran. Factors contributing to the widespread use of hawala are currency exchange restrictions and the large number of Iranian expatriates. The smuggling of goods into Afghanistan from Iran leads to a significant amount of trade-based money laundering. Goods purchased in Dubai are sent to one of many ports in southern Iran and then via land routes to other markets in Afghanistan and Pakistan. The goods imported into Iran and sent into Afghanistan are often part of the Afghan Transit Trade. Many of these goods are eventually found on the regional black markets. Iran is also a major transit route for opiates smuggled from Afghanistan.

In 2003, the Majlis (Parliament) passed an anti-money laundering act. The law includes customer identification requirements, mandatory record keeping for five years after the opening of accounts, and the reporting of suspicious activities. Iran is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. It has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

It does not have a law on terrorist financing. The Government of Iran should construct a viable anti-money laundering and terrorist financing regime that adheres to international standards. It should ratify the UN Convention against Transnational Organized Crime. It should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism. It should not support terrorism or the funding of terrorism.

Iraq

Iraq's economy is cash-based. The two state-owned banks control at least 90 percent of the banking sector. However, the sector is growing and at least 10 new banks, both domestic and international, have been licensed to operate in Iraq. Iraq has free trade zones in: Basra/Khor al-Zubair, Ninewa/Falafel, Sulaymaniyah, and Al-Quaymen. Under the Free Zone (FZ) Authority Law, goods imported and exported from the FZ are generally exempt from all taxes and duties, unless imported into Iraq. Additionally, capital, profits, and investment income from projects in the FZ are exempt from taxes and fees throughout the life of the project, including in the foundation and construction phases.

The Coalition Provisional Authority (CPA), the international body that governed Iraq beginning in April 2003, issued Regulations and Orders that carried the weight of law in Iraq. The CPA ceased to exist in June 2004, at which time the Iraqi Interim Government assumed authority for governing Iraq. Drafted and agreed by Iraqi leaders, the Transitional Administrative Law (TAL) describes the powers of the Iraqi government during the transition period. Under TAL Article 26, Regulations and Orders issued by the CPA pursuant to its authority under international law remain in force until rescinded or amended by legislation duly enacted and having the force of law. The constitution, which was ratified in October 2005 but which does not take effect until a permanent government is formed, also provides for the continuation of existing law, including CPA Regulations and Orders, until the existing law is annulled or amended in accordance with the constitution.

CPA Order No. 93, “Anti-Money Laundering Act of 2004” (AML Act), governs financial institutions in connection with: money laundering, financing of crime, financing terrorism, and the vigilance required of financial institutions in regard to financial transactions. The law also criminalizes money laundering, financing crime, including the financing of terrorism, and structuring transactions to avoid legal requirements. The AML Act covers: banks; asset, investment fund and securities dealers or managers; insurance entities; money transmitters and foreign currency exchanges, as well as persons who deal in financial instruments, precious metals or gems; and persons who undertake hawala transactions. Covered entities are required to verify the identity of any customer opening an account for any amount. Covered entities are also required to verify the identity of non-account holders performing a transaction or series of potentially related transactions whose value is equal to or greater than five million Iraqi dinar (approximately $3,500). Beneficial owners must be identified upon account opening or for transactions exceeding ten million Iraqi dinar (approximately $7,000). Records must be maintained for at least five years. Covered entities must report suspicious transactions and wait for guidance before proceeding with the transaction; the relevant funds are frozen until guidance is received. Suspicious transaction reports (STRs) are to be completed for all transactions over four million Iraqi dinar (approximately $3,000) that is believed to, for example, involve funds that are derived from illegal activities or money laundering, intended for the financing of crime, including terrorism, or over which a criminal organization has disposal power, or a transaction conducted to evade any law for which there is no apparent business or other lawful purpose. The “tipping off” of customers by bank employees where a transaction has generated a suspicious transaction report is prohibited. However, bank employees are protected from liability for cooperating with the government. Willful violations of the reporting requirement may result in imprisonment or fines.

CPA Order No. 94, “Banking Law of 2004,” gives the Central Bank of Iraq (CBI) the authority to license banks and to conduct due diligence on proposed bank management. Order No. 94 establishes requirements for bank capital, confidentiality of records, audit and reporting requirements for banks, and prudential standards. The CBI is responsible for the supervision of financial institutions. The CBI is mandated by the AML Act to issue regulations and require financial institutions to provide employee training, appoint compliance officers, develop internal procedures and controls to deter money laundering, and establish an independent audit function. The AML Act provides that the CBI will issue guidelines on suspicious financial activities and conduct on-site examinations to determine institutions’ compliance. The CBI also may issue regulations to require large currency transaction reports for the cross-border transport of currency of more than 15 million Iraqi dinar (approximately $10,000). Neither Iraqis nor foreigners are permitted to transport more than $10,000 in currency when exiting Iraq. The CBI is also mandated by the AML Act to distribute the UN 1267 Sanction Committee’s consolidated list of suspected terrorists or terrorist organizations. No asset freezes pertaining to any names on the consolidated list have been reported to date. Order No. 94 gives administrative enforcement authority to the CBI, up to and including the removal of institution management and revocation of bank licenses.

The AML Act calls for the establishment of the Money Laundering Reporting Office (MLRO) within the CBI. The MLRO has yet to become operational. The CBI and the USG are working together to build this capacity and implement the day-to-day functions of a financial intelligence unit (FIU). The MLRO will operate independently to collect, analyze and disseminate information on financial transactions subject to financial monitoring and reporting, including suspicious activity reports. The MLRO is also empowered to exchange information with other Iraqi or foreign government agencies.

The predicate offenses for the crimes of money laundering and the financing of crime are quite broad and extend beyond “all serious offenses” to include “some form of unlawful activity.” The penalties for violating the AML Act depend on the specific nature of the underlying criminal activity. For example, "money laundering" is punishable by a fine of up to 40 million dinar (approximately $27,080), or twice the value of the property involved in the transaction (whichever is greater), or imprisonment of up to four years, or both. Other offenses for which there are specific penalties include the financing of crime (a fine of up to 20 million dinar (approximately $13,540), two years' imprisonment, or both) and structuring transactions (up to 10 million dinar (approximately $6,770), one year imprisonment, or both). No arrests or prosecutions under the AML Act have been reported to date.

The AML Act also includes provisions for the forfeiture of any property, real or personal, including but not limited to funds involved in a covered offense, or any property traceable to the property, or any property gained as a result of such an offense, without prejudicing the rights of bona fide third parties. It also blocks any funds or assets, other than real property (which is covered by a separate regulation), belonging to members of the former Iraqi regime and authorizes the Minister of Finance to confiscate such assets following a judicial or administrative order. The lack of automation or infrastructure in the banking sector, however, hinders the government's ability to identify and freeze assets linked to illicit activity.

Iraq became a member of the Middle East and North Africa Financial Action Task Force (MENAFATF) in September 2005. Iraq is a party to the 1988 UN Drug Convention but not the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime. Iraq should ratify these conventions. It should take an active part in MENAFATF and implement its recommendations. Iraq should continue its efforts to build capacity and actively implement the provisions of the AML Act and related authorities. As a priority, Iraq, should establish the MLRO and FIU, as well as develop increased capacity to investigate financial crimes and enforce the provisions of the AML Act. In addition, it should ensure that any new legislation that either replaces or enhances the AML Act or the Banking Law meets current international standards.

Ireland

Narcotics trafficking, fraud, and tax offenses are the primary sources of funds laundered in Ireland. Money laundering mostly occurs in financial institutions such as bureaux de change. Additionally, investigations in Ireland indicate that some business professionals have specialized in the creation of legal entities, such as shell corporations, as a means of laundering money. Trusts are also established as a means of transferring funds from the country of origin to offshore locations. The use of shell corporations and trusts makes it more difficult to establish the true beneficiary of the funds, which makes it difficult to follow the money trail and establish a link between the funds and the criminal.

Suspicious Transaction Reports (STRs), received by the Revenue Commissioners and the Garda Bureau of Fraud Investigation (GBFI), cites the use of solicitors, accountants, and company formation agencies in Ireland to create shell companies. Investigations have disclosed that these companies are used to provide a series of transactions connected to money laundering, fraudulent activity, and tax offenses. The difficulties in establishing the beneficial owner have been complicated by the fact that the directors are usually nominees and are often principals of a solicitors' firm or a company formation agency.

Ireland criminalized money laundering relating to narcotics trafficking and other offenses in 1994. Financial institutions (banks, building societies, the Post Office, stockbrokers, credit unions, bureaux de change, life insurance companies, and insurance brokers) are required to report suspicious transactions and currency transactions exceeding approximately $15,000. The financial institutions are also required to implement customer identification procedures, and retain records of financial transactions. In 2003, Ireland amended its Anti-Money Laundering law to extend the requirements of customer identification and suspicious transaction reporting to lawyers, accountants, auditors, real estate agents, auctioneers, and dealers in high-value goods, thus aligning its laws with the Council Directive 2001/97/EC on prevention of the use of the financial system for money laundering (2nd EU Money Laundering Directive)

The Irish Financial Services Regulatory Authority (IFSRA) supervises the financial institutions for compliance with money laundering procedures. The Central Bank reports to the Irish Police regarding institutions under its supervision. The reports cover failure to establish identity of customers, failure to retain evidence of identification, and failure to adopt measures to prevent and detect the commission of a money laundering offense. In addition to STRs, there are customs reporting requirements for anyone transporting more than 12,700 euro (approximately $15,300).

Ireland's international banking and financial services sector is concentrated in Dublin's International Financial Services Centre (IFSC). In 2005, there were approximately 430 international financial institutions and companies operating in the IFSC. Services offered include banking, fiscal management, re-insurance, fund administration, and foreign exchange dealing. The IFSRA regulates the IFSC companies that conduct banking, insurance, and fund transactions. Tax privileges for IFSC companies were phased out over recent years and expired in 2005.

In 1999, the Corporate Law was amended to address problems arising from the abuse of Irish-registered nonresident companies (companies which are incorporated in Ireland, but do not carry out any activity in the country). The legislation requires that every company applying for registration must demonstrate that it intends to carry on an activity in the country. Companies must maintain at all times an Irish resident director or post a bond as a surety for failure to comply with the appropriate company law. In addition, the number of directorships that any one person can hold, subject to certain exemptions, is limited to 25. This is aimed at curbing the use of nominee directors as a means of disguising beneficial ownership or control.

In August 2001, the Government of Ireland (GOI) enacted the Company Law Enforcement Act 2001 (Company Act), to deal with problems associated with shell companies. The legislation establishes the Office of the Director of Corporate Enforcement (ODCE), whose responsibility it is to investigate and enforce the Company Act. The ODCE also has a general supervisory role in respect of liquidators and receivers. Under the law, the beneficial directors of a company have to be named. The Company Act also creates a mandatory reporting obligation for auditors to report suspicions of breaches of company law to the ODCE. In 2005, the ODCE had 16 prosecutions resulting in fines of varying amounts, four less than in 2004.

The Garda Bureau of Fraud Investigation (GBFI), Ireland's financial intelligence unit (FIU), analyzes financial disclosures. In 2003, a new Irish legal requirement went into effect, mandating that covered institutions file STRs with the Revenue (Tax) Department in addition to the BFI. Ireland estimates that up to 80 percent of STRs may involve tax violations. The Value Added Tax (VAT) fraud scams are the most prolific and have increased significantly in recent years. In 2004, the Criminal Assets Bureau took action in a number of such cases, the details of which are not yet available. The number of STRs filed increased from 4,254 in 2003 to 5,491 in 2004. Convictions for money laundering offenses under the Criminal Justice Act totaled four in 2001, two in 2002, and two in 2003. In 2004, there were seven prosecutions resulting in three convictions, currently awaiting sentencing. A conviction on charges of money laundering carries a maximum penalty of 14 years' imprisonment and an unlimited fine. To date, the strongest penalty applied for the conviction of money laundering is six years.

Under certain circumstances, the High Court can freeze, and, where appropriate, seize the proceeds of crimes. When criminal activity is suspected, the exchange of information between police and the Revenue Commissioner is authorized. The Criminal Assets Bureau (CAB) was established in 1996 to confiscate the proceeds of crime in cases where there is no criminal conviction. The CAB reports to the Minister for Justice and includes experts from Police, Tax, Customs, and Social Security Agencies.

Under the Proceeds of Crime Act 1996, specified property may be frozen for a period of seven years, unless the court is satisfied that all or part of the property is not the proceeds of crime. Since 1996, the CAB has frozen over 55 million euro of assets. In 2004, the CAB collected 16.4 million euro in taxes against the proceeds of criminal activity. In 2003, the CAB also initiated criminal prosecutions against a number of suspects for breaches of criminal law, and proceeded with successful investigations/prosecutions for revenue and social welfare offenses previously not presented before the criminal courts.

On March 9, the Irish government made strides in strengthening antiterrorism legislation when President Mary McAleese signed the Criminal Justice (Terrorism Offenses) Bill 2002 into law. This legislation brought Ireland in line with United Nations Conventions and European Union Framework decisions on combating terrorism. It enabled Ireland to ratify and accede to the remaining four UN conventions on terrorism. (Ireland had previously acceded to eight of twelve) and significantly strengthened the government's ability to seize assets and prosecute those suspected of supporting terrorism. Until this law passed, GOI authorities could pursue and prosecute suspects of terrorism, notably terrorism financing, only if they also had committed criminal offenses in Ireland or had been designated by the UN 1267 Sanctions Committee's consolidated list or by the EU. Implementation of the new anti terrorism legislation and its anti-money laundering law amendments, plus stringent enforcement of all such initiatives, will enhance Ireland's efforts to maintain an effective anti-money laundering program. The Central Bank, moreover, participates with the Irish Parliament subcommittee in drafting guidance notes for regulated institutions on combating and preventing terrorist financing. These notes were revised and issued to institutions upon the passing of the bill.

The law allows the Irish Police to apply to the courts to freeze assets where certain evidentiary requirements are met. Ireland reported to the European Commission the names of seven individuals, the most recent one in 2004, who maintained a total of nine accounts that were frozen in accordance with the provisions of the European Union's (EU) Anti-Terrorist Legislation. The aggregate value of the funds frozen is approximately 90,000 euro (approximately $109,000).

In February seven people from the Republic of Ireland were arrested in a police raid on suspects believed to be laundering some of the 26.5 pounds sterling (38 million euro- approximately $45,260,000) stolen from the Northern Bank, Belfast on December 23, 2004. Over 2.3m pounds sterling and 94,000 (approximately $120,000) euro was seized in Cork and Dublin. Up to 100 officers from the Criminal Assets Bureau, Garda Bureau of Fraud Investigation, Special Detective Unit and Crime and Security Section were involved in the arrests, with no charges filed, or prosecutions begun.

In July, the United States and Ireland signed instruments on extradition and mutual legal assistance. These instruments are part of a sequence of bilateral agreements that the United States is concluding with all 25 EU Member States, in order to implement twin agreements on extradition and mutual legal assistance with the European Union in 2003. The instruments signed by Ireland will supplement and update the 1983 U.S.-Ireland extradition treaty and the 2001 bilateral treaty on mutual legal assistance (MLAT). The 1983 extradition treaty between Ireland and the U.S. is in force, while the ratification process for the 2001 MLAT has not yet been completed by the GOI. Regarding mutual assistance, the instruments provide for searches of suspect foreign located bank accounts, joint investigative teams, and testimony by video-link.

Ireland is a member of the EU, and the FATF. The FIU is a member of the Egmont Group. Ireland is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the 1988 UN Drug Convention. Ireland is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

"Shell" companies-companies that have no physical presence and normally have nominee directors are contrary to FATF's international standards. These "paper companies" are convenient vehicles for the laundering of funds and could be used to finance terrorism. The GOI should consider strengthening measures to prevent the establishment of such companies. Similarly, law enforcement should have a stronger role in identifying the true beneficial owners of shell companies as well as of trusts in the course of investigations.

Isle of Man

The Isle of Man (IOM) is a Crown Dependency of the United Kingdom located between England and Ireland in the Irish Sea. Its large and sophisticated financial center is potentially vulnerable to money laundering at the layering and integration stages. The U.S. dollar is the most common currency used for criminal activity in the IOM. Most of the illicit funds in the IOM are from fraud schemes and narcotics trafficking in other jurisdictions, including the United Kingdom. Identity theft and Internet abuse are growing segments of financial crime activity.

As of September 30, 2004, the IOM's financial industry consisted of approximately 19 life insurance companies, 25 insurance managers, more than 177 captive insurance companies, more than 17.2 billion pounds (approximately $32.7 billion) in life insurance funds and 5.6 billion pounds (approximately $10.6 billion) in non-life insurance funds under management, 53 licensed banks and two licensed building societies, 82 investment business license holders, 30.1 billion pounds (approximately $57.2 billion) in bank deposits, and 164 collective investment schemes with 6.5 billion pounds (approximately $12.4 billion) of funds under management. There are also 171 licensed corporate service providers, with approximately another seven seeking licenses.

Money laundering related to narcotics trafficking was criminalized in 1987. The Prevention of Terrorism Act 1990 made it an offense to contribute to terrorist organizations, or to assist a terrorist organization in the retention or control of terrorist funds. In 1998, money laundering arising from all serious crimes was criminalized. Financial institutions and professionals such as banks, fund managers, stockbrokers, insurance companies, investment businesses, credit unions, bureaux de change, check cashing facilities, money transmission services, real estate agents, auditors, casinos, accountants, lawyers, and trustees are required to report suspicious transactions and comply with the requirements of the anti-money laundering (AML) code, such as customer identification.

The Financial Supervision Commission (FSC) and the Insurance and Pension Authority (IPA) regulate the IOM financial sector. The FSC is responsible for the licensing, authorization, and supervision of banks, building societies, investment businesses, collective investment schemes, corporate service providers, and companies. The IPA regulates insurance companies, insurance management companies, general insurance intermediaries, and retirement benefit schemes and their administrators. In addition, the FSC also maintains the Company Registry Database for the IOM, which contains company records dating back to the first company incorporated in 1865. Statutory documents filed by IOM companies can now be searched and purchased online through the FSC's website.

Instances of failure to disclose suspicious activity would result in both a report being made to the Financial Crimes Unit (FCU), the IOM's financial intelligence unit (FIU), and possible punitive action by the regulator, which could include revoking the business license. To assist license holders in the effective implementation of anti-money laundering techniques, the regulators hold regular seminars and additional workshop training sessions in partnership with the FCU and the Isle of Man Customs and Excise.

In December 2000, the FSC issued a consultation paper, jointly with the Crown Dependencies of Guernsey and Jersey, called Overriding Principles for a Revised Know Your Customer Framework, to develop a more coordinated approach on anti-money laundering. Further work between the Crown Dependencies is being undertaken to develop a coordinated strategy on money laundering, to ensure compliance as far as possible with the revised Financial Action Task Force (FATF) Forty

Recommendations on Money Laundering. The IOM is also assisting the FATF Working Groups considering matters relating to customer identification and companies' issues.

In August 2002, money service businesses (MSBs) not already regulated by the FSC or IPA were required to register with Customs and Excise. This implemented the 1991 EU Directive on Money Laundering, revised by the Second Directive 2001/97/EC, for MSBs and provides for their supervision by Customs and Excise to ensure compliance with the AML Codes.

The IPA, as regulator of the IOM's insurance and pensions business, issues Anti-Money Laundering Standards for Insurance Businesses (the "Standards"). The Standards are binding upon the industry and include the Overriding Principles. These include a requirement that all insurance businesses check their whole book of businesses to determine that they have sufficient information available to prove customer identity. The current set of Standards became effective March 31, 2003. In addition, the IPA conducts on-site visits to examine procedures and policies of companies under its supervision.

The Online Gambling Regulation Act 2001 and an accompanying AML (Online Gambling) Code 2002 are supplemented by AML guidance notes issued by the Gambling Control Commission, a regulatory body which provides more detailed guidance on the prevention of money laundering through the use of online gambling. The Online Gambling legislation brought regulation to what was technically an unregulated gaming environment. The dedicated Online Gambling AML Code was at the time unique within this segment of the gambling industry.

The Companies, Etc. (Amendment) Act 2003 calls for additional supervision for all licensable businesses, e.g., banking, investment, insurance and corporate service providers. The act further provides that no future bearer shares will be issued after April 1, 2004, and all existing bearer shares must be registered before any rights relating to such shares can be exercised.

The FCU, formed in April 2000, evolved from the police Fraud Squad and now includes both police and customs staff. It is the central point for the collection, analysis, investigation, and dissemination of suspicious transaction reports (STRs) from obligated entities. The entities required to report suspicious transactions include banks/financial institutions, bureaux de change. casinos, post offices, lawyers, accountants, advocates, and businesses involved with investments, insurance, real estate, gaming/lotteries, and money changers. The FIU received 2,265 suspicious transaction reports (STRs) in 2005, 2,315 STRs in 2004, and 1,920 STRs in 2003. In 2005, the FIU referred approximately 11 percent of the STRs to the United Kingdom, two percent to other European jurisdictions and 12 percent to non-European jurisdictions as referrals to law enforcement for investigation. In 2004, the FIU referred 19 percent of the STRs to the United Kingdom, eight percent to Europe and 31 percent to non-European jurisdictions. There is no minimum threshold for obligated entities to file a STR and reporting individuals (compliance officers, bankers, etc.) are protected by law when filing suspicious transactions.

The FCU is organized under the Department of Home Affairs. The FIU has access to Customs, police and tax information. The STRs are disseminated through agreements to the IOM Customs, Tax Administrators, Financial Supervision Commission (FSC) and the Insurance and Pension Authority (IPA). The FCU is responsible for investigating financial crimes and terrorist financing cases. In 2005, there were four arrests and one prosecution for money laundering involving narcotics.

The Criminal Justice Acts of 1990 and 1991, as amended, extend the power to freeze and confiscate assets to a wider range of crimes, increase the penalties for a breach of money laundering codes, and repeal the requirement for the Attorney General's consent prior to disclosure of certain information. Assistance by way of restraint and confiscation of assets of a defendant is available under the 1990 Act to all countries and territories designated by Order under the Act, and the availability of such assistance is not convention-based nor does it require reciprocity. Assistance is also available under the 1991 Act to all countries and territories in the form of the provision of evidence for the purposes of criminal investigations and proceedings.

Under the 1990 Act the provision of documents and information is available to all countries and territories for the purposes of investigations into serious or complex fraud. Similar assistance is also available to all countries and territories in relation to drug trafficking and terrorist investigations. All decisions for assistance are made by the Attorney General of the IOM on a case-by-case basis, depending on the circumstances of the inquiry. The law also addresses the disclosure of a suspicion of money laundering. Since June 2001, it has been an offense to fail to make a disclosure of suspicion of money laundering for all predicate crimes, whereas previously this just applied to drug- and terrorism-related crimes. The law also lowers the standard for seizing cash from "reasonable grounds" to believe that it was related to drug or terrorism crimes to a "suspicion" of any criminal conduct. The law also provides powers to constables, including customs officers, to investigate whether a person has benefited from any criminal conduct. These powers allow information to be obtained about that person's financial affairs. These powers can be used to assist in criminal investigations abroad as well as in the IOM.

The United Kingdom implemented the amendments to its Proceeds of Crime Act in 2004. The IOM is currently reviewing new legislation that will redo its Criminal Justice Act along similar lines. The new amendments are under consideration and are expected to come into force in late 2005 or early 2006.

The Customs and Excise (Amendment) Act 2001 gives various law enforcement and statutory bodies within the IOM the ability to exchange information, where such information would assist them in discharging their functions. The Act also permits Customs and Excise to release information it holds to any agency within or outside the IOM for the purposes of any criminal investigation and proceeding. Such exchanges can be either spontaneous or by request.

The Government of the IOM enacted the Anti-Terrorism and Crime Act, 2003. The purpose of the Act is to enhance reporting, by making it an offense not to report suspicious transactions relating to money intended to finance terrorism. The IOM Terrorism (United Nations Measure) Order 2001 implements UNSCR 1373 by providing for the freezing of terrorist funds, as well as by creating a criminal offense with respect to facilitators of terrorism or its financing. All charities are registered and supervised by the Charities Commission. All other UN and EU financial sanctions have been adopted or applied in the IOM, and are administered by Customs and Excise. Institutions are obliged to freeze affected funds and report the facts to Customs and Excise. The FSC's anti-money laundering guidance notes have been revised to include information relevant to terrorist events. The Guidance Notes were issued in December 2001. Additional amendments are being reviewed that will incorporate the new FATF recommendations and EU directives.

The IOM has developed a legal and constitutional framework for combating money laundering and the financing of terrorism. There appears to be a high level of awareness of anti-money laundering and counterterrorist financing issues within the financial sector, and considerable effort has been made to put appropriate practices into place. In November 2003, the Government of the IOM published the full report made by the International Monetary Fund (IMF) following its examination of the regulation and supervision of the IOM's financial sector. In this report the IMF commends the IOM for its robust regulatory regime. The IMF found that "the financial regulatory and supervisory system of the Isle of Man complies well with the assessed international standards." The report concludes the Isle of Man fully meets international standards in areas such as banking, insurance, securities, anti-money laundering, and combating the financing of terrorism.

The IOM is a member of the Offshore Group of Banking Supervisors. The IOM is also a member of the International Association of Insurance Supervisors and the Offshore Group of Insurance Supervisors. The FCU belongs to the Egmont Group. The IOM cooperates with international anti-money laundering authorities on regulatory and criminal matters. Application of the 1988 UN Drug Convention was extended to the IOM in 1993.

Isle of Man officials should continue to support and educate the local financial sector to help it combat current trends in money laundering. The authorities also should continue to work with international anti-money laundering authorities to deter financial crime and the financing of terrorism and terrorists.

Israel

Israel is not a regional financial center. It primarily conducts financial activity with the financial markets of the United States and Europe, and to a lesser extent with Asia. Less than a quarter of all Israeli money laundering or terrorist financing seizures are related to narcotics proceeds. The majority of the seizures are related to fraud, theft, embezzlement, and illegal money services providers (MSP). Most significant criminal activities that were investigated in 2005 were related to intentional false property transactions reporting. Israel does not have free trade zones and is not considered an offshore financial center.

Israel enacted the "Prohibition on Money Laundering Law" (PMLL) on August 8, 2000 (Law No. 5760-2000). The PMLL established a framework for an anti-money laundering system, but required the passage of several implementing regulations before the law could fully take effect. Among other things, the PMLL criminalized money laundering and included more than 18 serious crimes, in addition to offenses described in the prevention of terrorism ordinance, as predicate offenses for money laundering.

In addition, Israel adopted in 2001 the "Prohibition on Money Laundering (The Banking Corporations Requirement Regarding Identification, Reporting, and Record Keeping) Order." The Order establishes specific procedures for banks with respect to customer identification, record keeping, and the reporting of irregular and suspicious transactions. The PMLL requires the declaration of currency transferred (including cash, travelers' checks, and banker checks) into or out of Israel for sums above 80,000 new Israeli shekels (nis) (about $17,200). This applies to any person entering or leaving Israel and to any person bringing or taking money into or out of Israel by mail or by any other methods, including cash couriers. This offense is punishable by up to six months' imprisonment or a fine of nis 202,000 ($43,400), or ten times the amount that was not declared, whichever is higher. Alternatively, an administrative sanction of nis 101,000 ($21,700), or five times the amount that was not declared, may be imposed. In 2003, the Government of Israel (GOI) lowered the threshold for reporting cash transaction reports (CTRs) to nis 50,000 ($10,500), lowered the document retention threshold to nis 10,000 ($2,100), and imposed more stringent reporting requirements.

The PMLL also provided for the establishment of the Israeli Money Laundering Prohibition Authority (IMPA) as the country's financial intelligence unit (FIU). IMPA became operational in 2002. The PMLL requires financial institutions to report "unusual transactions" to IMPA as soon as possible under the circumstances. The term "unusual transactions" is loosely defined. However, it is used so that the IMPA will receive reports even when the financial institution is unable to link the unusual transaction with money laundering. In addition, suspicious transaction reporting is required of members of the stock exchange, portfolio managers, insurers or insurance agents, provident funds and companies managing a provident fund, providers of currency services, and the Postal Bank. The PMLL does not apply to intermediaries such as lawyers and accountants.

In 2002, Israel enacted several new amendments to the PMLL that resulted in the addition of the money services businesses (MSB) to the list of entities required to file cash transaction reports (CTRs) and suspicious transaction reports (STRs), the establishment of a mechanism for customs officials to input into the IMPA database, the creation of regulations stipulating the time and method of bank reporting, and the creation of rules on safeguarding the IMPA database and rules for requesting and transmitting information between IMPA, the Israeli National Police (INP) and the Israel Security Agency. The PMLL also authorized the issuance of regulations requiring financial service providers to identify, report, and keep records for specified transactions for seven years.

The Financial Action Task Force (FATF) removed Israel from its Non-Cooperative Countries and Territories (NCCT) list in June 2002. A U.S. advisory issued by the Department of Treasury's Financial Crimes Enforcement Network in 2000 to U.S. financial institutions, emphasizing the need for enhanced scrutiny of certain transactions and banking relationships in Israel to ensure that appropriate measures are taken to minimize risk for money laundering, was also withdrawn in 2002. That same year, IMPA was admitted into the Egmont Group of financial intelligence units.

The PMLL mandates the registration of MSBs through the Providers of Currency Services Registrar at the Ministry of Finance. In 2004, Israeli courts convicted several MSBs for failure to register with the Registrar of Currency Services. In addition, several criminal investigations have been conducted against other currency-services providers, some of which have resulted in money laundering indictments, which are still pending. The closure of unregistered MSBs was a priority objective of the INP in 2004, and it raided at least 19 such locations. The INP and the Financial Service Providers Regulatory Authority maintain a high level of coordination, routinely exchange information, and have conducted multiple joint enforcement actions. In the past year, Israeli courts convicted several MSBs for violating the obligation to register with the Registrar of Currency Services. In addition, several criminal investigations were brought against other MSBs, some of which resulted in money laundering indictments that are still pending criminal trials.

The Israeli National Police (INP) reports no indications of an overall increase in financial crime relative to previous years. However, during 2005, Israel has been the nexus of several high profile money laundering cases. In March 2005, the International Crimes Unit (ICU) of the Israeli National Police (INP) raided Bank Hapoalim and its trust company, in what was described as the biggest money laundering scandal ever in Israel. The police froze over 180 accounts with more than $376 million, and some 24 employees were detained, including the manager and four senior executives. The operation came to light with information obtained by the ICU. In addition, the police arrested an Israeli citizen in March in connection with what is considered to be one of the largest robbery attempts in British history. Hackers planned to steal about $450 million from a Japanese bank in London, and then launder part of the funds through a bank account that belonged to the Israeli citizen's company.

The legislative regime criminalizing the financing of terrorism includes provisions of the defense regulations (state of emergency) (1945), the prevention of terrorism ordinance (1948), the penal law (1977), and the PMLL. On December 29, 2004, the Israeli parliament adopted the prohibition on terrorist financing law 5765-2004, which is geared to further modernize and enhance Israel's ability to combat terrorist financing and to cooperate with other countries on such matters. This law went into effect in August 2005. Under the International Legal Assistance Law of 1998, Israeli courts are empowered to enforce forfeiture orders executed in foreign courts for crimes committed outside Israel. The new anti-money laundering law has recently enhanced this ability.

Israel has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets, as well as assets derived from or intended for other serious crimes, including the funding of terrorism. The identification and tracing of such assets is part of the ongoing function of the Israeli intelligence authorities and IMPA. In 2005, 6,005 suspicious transaction reports were received by IMPA. During this period IMPA disseminated several hundred intelligence reports to law enforcement agencies in response to requests. In addition, twelve different investigations yielded indictments (some of them multiple indictments). In another case, prosecutors indicted a number of bank officials for money laundering offenses for violation of the obligation to report unusual transactions and for advising their customers on ways of avoiding reporting to IMPA. In 2005, the INP seized approximately $75 million in suspected criminal assets. Total seizures for each of the previous three years ranged from $23-$27 million each year.

Israel is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Israel signed the UN Convention against Transnational Organized Crime on December 13, 2000, but has not yet ratified it. In June 2003, the Knesset adopted the Combating Criminal Organizations Law, which includes comprehensive measures with regard to organized crime. On November 29, 2005, Israel signed the United Nations Convention against Corruption.

The Government of Israel continued to make progress in strengthening its anti-money laundering and terrorist financing regime in 2005. Israel has entered into several bilateral agreements and memoranda of understanding aimed at combating financial crimes. However, there is a continuing need for more effective bank supervision and proactive investigations of money laundering associated with criminal activity, especially on the part of organized crime figures and syndicates.

Israel should also examine the misuse of the international diamond trade to launder funds. Israel should continue to enforce regulations pursuant to the PMLL and continue improving its anti-money laundering and counterterrorist financing regime through ensuring the diligent reporting of suspicious activities by banks and non-financial institutions. Israel should ratify the UN Convention against Transnational Organized Crime.

Italy

Italy is not an important regional or offshore financial center. However, money laundering is a concern both because of the prevalence of homegrown organized crime groups and the recent influx of criminal organizations from abroad, especially from Albania, Romania, and Russia. Counternarcotics efforts are complicated by the heavy involvement in international narcotics trafficking of domestic and Italian-based foreign organized crime groups. Italy is a consumer country and a major transit point for heroin coming from the Near East and Southwest Asia through the Balkans en route to Western/Central Europe and, to a lesser extent, the United States. Italian and ethnic Albanian criminal organizations work together to funnel drugs to and through Italy. Additional priority trafficking groups include other Balkan organized crime entities, as well as Nigerian, Dominican, and Colombian and other South American trafficking groups. In addition to the narcotics trade, laundered funds come from a myriad of criminal activities, such as alien smuggling, contraband cigarette smuggling, pirated goods, extortion, usury, and kidnapping. Financial crimes not directly linked to money laundering, such as credit card and Internet fraud, are increasing.

Money laundering occurs both in the regular banking sector and, more frequently, in the non-bank financial system, i.e., casinos, money transfer houses, and the gold market. Money launderers predominantly use non-bank financial institutions for the illicit export of currency—primarily U.S. dollars and euros—to be laundered in offshore companies. There is a substantial black market for smuggled goods in the country, but it is not funded significantly by narcotics proceeds.

Money laundering is defined as a criminal offense when it relates to a separate, intentional felony offense. All intentional criminal offenses are predicates to the crime of money laundering, regardless of the applicable sentence for the predicate offense. Italy has strict laws on the control of currency deposits in banks. Banks must identify their customers and record and report to the Italian exchange office (UIC)—Italy's financial intelligence unit (FIU)—any cash transaction that exceeds approximately $15,000. The Bank of Italy's mandatory guidelines require the reporting of all suspicious cash transactions and other activity—such as a third party payment on an international transaction—on a case-by-case basis. Italian law prohibits the use of cash or negotiable bearer instruments for transferring money in amounts in excess of approximately $15,000, except through authorized intermediaries/brokers.

Banks and other financial institutions are required to maintain for ten years records necessary to reconstruct significant transactions, including information about the point of origin of funds transfers and related messages sent to or from Italy. Banks operating in Italy must remit account data to a central archive controlled by the Bank of Italy. This archive was established for record keeping and financial oversight purposes, but has proved useful for tracking money laundering. A "banker negligence" law makes individual bankers responsible if their institutions launder money. The law protects bankers and others with respect to their cooperation with law enforcement.

Italy has addressed the problem of international transportation of illegal-source currency and monetary instruments by applying the $15,000-equivalent reporting requirement to cross-border transport of domestic and foreign currencies and negotiable bearer instruments. Reporting is mandatory for cross-border transactions involving negotiable bearer monetary instruments (e.g., checks), but not for wire transfers; nevertheless, financial institutions are required to maintain a uniform anti-money laundering database for wire transfers and to submit this data on a monthly basis to the UIC. During 2004, the last year for which complete figures are available, the UIC received 6,816 suspicious transaction reports (STRs) related to money laundering and 288 related to the financing of terrorism. The UIC itself does little filtering of the STRs, but rather sends virtually all of them to the Anti-Mafia Investigative Unit (DIA) and the Guardia di Finanza (GdF), Italy's financial police. During 2004, law enforcement opened 328 investigations based on STRs, which resulted in 103 prosecutions.

Because of Italy's strong banking controls, narcotics traffickers are using different ways of laundering drug proceeds. To deter nontraditional money laundering, the Government of Italy (GOI) has enacted a decree to broaden the category of institutions and professionals required to abide by anti-money laundering regulations. The list now includes debt collectors, exchange houses, insurance companies, casinos, real estate agents, brokerage firms, gold and valuables dealers and importers, auction houses, art galleries, antiques dealers, labor advisors, lawyers, and notaries. Not all implementing regulations for the decree have been issued, so while Italy has comprehensive internal auditing and training requirements for its (broadly-defined) financial sector, implementation of these measures by non-bank financial institutions lags behind that of banks, as evidenced by the relatively low number of STRs filed by non-bank financial institutions. According to UIC data, banking institutions submit 88 per cent of all STRs. Other financial intermediaries such as exchange houses submit 5.5 per cent, insurance companies 3.1 per cent, the postal sector 2.6 per cent, and all other sectors less than one per cent.

The UIC, which is an arm of the Bank of Italy, receives and analyzes STRs filed by covered institutions, and then forwards them to the National Anti-Mafia Directorate (local public prosecutors), the Anti-Mafia Directorate, or the GdF for further investigation. The UIC compiles a register of financial and non-financial intermediaries that carry on activities that could be vulnerable to money laundering. The UIC also performs supervisory and regulatory functions such as issuing decrees, regulations, and circulars. It does not require a court order to compel supervised institutions to provide details on regulated transactions.

A special currency unit of the GdF is the Italian law enforcement agency with primary jurisdiction for conducting financial investigations in Italy. STRs led the GdF to identify $14,400,000 in laundered money in 2003. Both the UIC and the special currency unit have access to the Bank of Italy's central archive. Investigators from other divisions in the GdF and other Italian law enforcement agencies must obtain a court order prior to being granted access to the archive.

Italy has established reliable systems for identifying, tracing, freezing, seizing, and forfeiting assets from narcotics trafficking and other serious crimes, including terrorism. These assets include currency accounts, real estate, vehicles, vessels, drugs, legitimate businesses used to launder drug money, and other instruments of crime. Under anti-Mafia legislation, seized financial and non-financial assets of organized crime groups can be forfeited. The law allows for forfeiture in both civil and criminal cases. Italy does not have any significant legal loopholes that allow traffickers and other criminals to shield assets. However, the burden of proof is on the Italian government to make a case in court that assets are related to narcotics trafficking or other serious crimes. Law enforcement officials have adequate powers and resources to trace and seize assets; however, their efforts can be affected by which local magistrate is working a particular case. Funds from asset forfeitures are entered into the general State accounts. Italy shares assets with member states of the Council of Europe. The GOI is currently involved in multilateral negotiations with the European Union (EU) to enhance asset tracing and seizure.

In October 2001, Italy passed a decree (subsequently converted into legislation) that created the Inter-Ministerial Financial Security Committee (FSC), which is charged with coordinating GOI efforts to track and interdict terrorist financing. The committee includes representatives from the Economics, Justice, and Foreign Affairs Ministries; law enforcement agencies; and the intelligence services. The Committee has far-reaching powers that include waiving provisions of the Official Secrecy Act to obtain information from all government ministries and the as-yet-unused authority to order a freeze of terrorist-related assets.

A second October 2001 decree (also converted into legislation) made financing of terrorist activity a criminal offense, with prison terms of between seven and 15 years. The legislation also requires financial institutions to report suspicious activity related to terrorist financing. Both measures facilitate the freezing of terrorist assets. The GOI cooperates fully with efforts by the United States to trace and seize assets. Italy is second only to the United States in the number of suspected terrorists and terrorist organizations it has submitted to the UNSCR 1267 Sanctions Committee for designation. The UIC transmits to financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 as well as those designated by the EU. The UIC may provisionally suspend for 48 hours transactions deemed suspect. The courts must then act to freeze or seize the assets. Under Italian law, financial and economic assets linked to terrorists can only be seized through a criminal sequestration order. Courts may issue such orders as part of criminal investigation of crimes linked to international terrorism. The sequestration order may be issued with respect to any asset, resource, or item of property, provided that these are goods or resources linked to the criminal activities under investigation. A provision of the Italian implementing legislation of the third EU money laundering directive would give the GOI the authority to issue a decree law allowing the freezing, seizing, and forfeiture of non-financial assets belonging to terrorist groups and individuals. This legislation ahs not yet been enacted by the Parliament. In Italy, the term "alternative remittance system" refers to non-bank regulated institutions such as money transfer businesses. Informal remittance systems do exist, primarily to serve Italy's significant immigrant communities. Italy does not regulate charities per se. Primarily for tax purposes, Italy in 1997 created a category of "not-for-profit organizations of social utility" (ONLUS). Such an organization can be an association, a foundation or a fundraising committee. To be classified as an ONLUS, the organization must register with the Economics Ministry and prepare an annual report. There are currently 19,000 registered ONLUS. The ONLUS Agency was established in 2000 and has the power to issue guidelines and to draft legislation for the non-profit sector; to maintain data and statistics; to alert other authorities in cases of violation of existing obligations; and to mandate delistings from the ONLUS registry. The ONLUS Agency recently launched a $240,000 project for the creation of a centralized database, to gather mandatory information related to all Italian ONLUS. The ONLUS Agency has reviewed 1,500 ONLUS and recommended the dissolution of several that were not in compliance with Italian law. Italian authorities believe that, based on analysis by the UIC and on investigations by the GdF, the risk of terrorist financing in the Italian non-profit sector is low.

Italian cooperation with the United States on money laundering matters has been exemplary. The United States and Italy have signed a customs assistance agreement as well as extradition and Mutual Legal Assistance treaties (MLAT). Both in response to requests under the MLAT and on an informal basis, Italy provides the United States records related to narcotics trafficking, terrorism and terrorist financing investigations and proceedings. Italy also cooperates closely with U.S. law enforcement agencies and other governments investigating illicit financing related to these and other serious crimes. The MLAT provides a basis for the United States to forfeit and share assets with Italy, but Italian law currently precludes Italy from reciprocating.

Italy is a party to the 1988 UN Drug Convention; the UN International Convention for the Suppression of the Financing of Terrorism; and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Italy has signed, but not yet ratified, the UN Convention Against Transnational Organized Crime.

Italy is a member of the Financial Action task Force (FATF) and held the FATF presidency in 1997-98. As a member of the Egmont Group, Italy's UIC shares information with other countries' FIUs. The UIC has been authorized to conclude information-sharing agreements concerning suspicious financial transactions with other countries. To date, Italy has signed memoranda of understanding with France, Spain, the Czech Republic, Croatia, Slovenia, Belgium, Panama, Latvia, the Russian Federation, Canada, and Australia. Italy also is negotiating agreements with Japan, Argentina, Malta, Thailand, Singapore, Hong Kong, Malaysia, and Switzerland, and has a number of bilateral agreements with foreign governments in the areas of investigative cooperation on narcotics trafficking and organized crime. There is no known instance of refusal to cooperate with foreign governments.

Italy is firmly committed to the fight against money laundering and terrorist financing, both domestically and internationally. However, given the relatively low number of STRs being filed by non-bank financial institutions, the GOI should increase its training efforts and supervision in this sector, to decrease its vulnerability to abuse by criminal or terrorist groups. Italy should also continue its active participation in multilateral fora dedicated to the global fight against money laundering and terrorist financing. It should ratify the UN Convention Against Transnational Organized Crime.

Jamaica

Jamaica, the foremost producer and exporter of marijuana in the Caribbean, is also a major transit country for cocaine flowing from South America to the United States and other international destinations. The profits from these significant illegal drug flows must be legitimated and therefore make Jamaica susceptible to money laundering activities and other financial crimes. Reportedly, Jamaican authorities have seen evidence that persons involved in the drug trade have been trying to legitimize their operations by establishing commercial enterprises and attempting to launder funds through real property transactions. There is a significant black market for smuggled goods, which is due to tax evasion.

Jamaica is not an offshore financial center and its banking system continues to be under intense scrutiny from regulators in the wake of several major banking scandals that surfaced in the 1990s. Because of this scrutiny, Jamaican financial instruments are considered an unattractive mechanism for laundering money. As a result, much of the proceeds from drug-trafficking and other criminal activity are used to acquire tangible assets such as real estate or luxury cars, while still more merely pass through Jamaica in the form of cash shipments to South America. Further complicating the picture are the hundreds of millions of U.S. dollars in remittances sent home to Jamaica by the substantial Jamaican population overseas.

The Government of Jamaica (GOJ) does not encourage or facilitate money laundering, nor has any senior official been investigated or charged with the laundering of proceeds from illegal activity.

The Money Laundering Act (MLA), implemented on January 5, 1998, governs Jamaica's anti-money laundering regime. The MLA criminalizes narcotics-related money laundering and introduces record keeping and reporting requirements for financial institutions on all currency transactions over $10,000. Exchange bureaus have a reporting threshold of $8,000. The MLA was amended in March 1999 to raise the threshold to $50,000, after complaints from financial sector institutions that had difficulties with the amount of paperwork resulting from the $10,000 threshold. At that time, a requirement was also added for banks to report suspicious transactions of any amount to the Director of Public Prosecutions (DPP). In February 2000, the MLA was amended to add fraud, firearms trafficking, and corruption as predicate offenses for money laundering. Jamaica is in the process of further amending and modernizing the MLA.

The GOJ is also attempting to pass the Proceeds of Crime Act that will enable it to identify, trace, freeze, seize and forfeit narcotics related assets as well as assets derived from other serious crimes. The major provisions of this legislation include all property or assets associated with an individual convicted or suspected of involvement with a crime. This includes legitimate businesses used to launder drug money or support terrorist activity. Currently, the Financial Investigations Division (FID) of the Ministry of Finance and the Jamaica Constabulary Force (JCF) are the entities responsible for tracing and seizing assets. The proceeds go to the forfeited asset fund.

During 2004, the Jamaican Parliament passed amendments to the Bank of Jamaica Act, the Banking Act, the Financial Institution Act and the Building Society Act that govern the periodic examination of commercial banks and financial institutions. The Acts provide the legal and policy parameters for the licensing and supervision of financial institutions and lay the foundation for the proposed amendments to the MLA.

In addition to a new Customs arrival form that requires declaration of currency or monetary instruments over $10,000 (or its equivalent) that was introduced in 2003, the GOJ changed its immigration form in conjunction with the implementation of a new border security entry/exit system designed to better control the flow of persons in and out of Jamaica. This measure should assist law enforcement efforts to combat the movement of large amounts of cash—often in shipments totaling hundreds of thousands of U.S. dollars through Jamaica. Jamaica has identified cash couriers violating the law and forfeited the cash. Cash smuggling reports are shared between government agencies.

There are two free trade zones that operate in Jamaica, one in Montego Bay and one in Kingston. Due to the demise of the garment industry, the free trade zones are mostly used for warehousing. There are plans to change the operations of the Kingston free zone into a base for logistic services and make Kingston a distribution hub for goods. The Montego Bay free zone is expected to become a major business center and position itself as a call center, focusing on information communication technology.

The FID consists of 14 forensic examiners, six police officers who have full arrest powers, a director and 5 administrative staff. The FID receives, analyses, and disseminates information. Matters requiring investigation are referred to the Financial Crimes Unit which is not a regulatory body. The FID also has responsibility for investigating financial crimes including money laundering and terrorist financing. They are adequately staffed and trained to fulfill their responsibilities.

If the Proceeds of Crime Act and Financial Investigation Division Act are passed, they are expected to lead to additional sharing of information. The Financial Investigation Unit (FIU), part of the FID, has discussed membership in the Egmont Group with Canadian authorities who have agreed to sponsor Jamaica's application.

Jamaica has an on-going continuing education program to ensure compliance with the suspicious transaction reporting (STR) requirements and mandatory reporting of suspicious transactions. The Bank of Jamaica supervises compliance. The FID reports that non-banking financial institutions have a seventy percent compliance rate with money laundering controls. Reporting individuals are protected by law with respect to their cooperation with law enforcement entities. STRs were filed in 2005 by: banks (125), currency exchanges (355), investment/securities dealers (8), merchant banks (3), building societies (84), credit unions (7) and remittance companies (6,828). The FID claims that the high number of STRs submitted by remittance companies is due to their lack of knowledge of the threshold limits.

June 15, 2005 marked Jamaica's first money laundering conviction. Further action is still required in the area of asset forfeiture. Law enforcement authorities are hampered by the fact that Jamaica has no civil forfeiture law, and under the 1994 Drug Offenses (Forfeiture of Proceeds) Act, a criminal drug-trafficking conviction is required as a prerequisite to forfeiture. This often means that even when police discover illicit funds, the money cannot be seized or frozen and must be returned to the criminals. Assets that are eventually forfeited are deposited into a fund shared by the Ministries of National Security, Justice and Finance. In 2004, GOJ agencies shared $85,000 from seizures from drug-trafficking, money laundering, tax and customs evasion and larceny. The new Proceeds of Crime Act, currently circulating in Parliament, will go a long way to address the shortcomings but the legislative process is moving slowly.

The Terrorism Prevention Act of 2005 criminalizes the financing of terrorism consistent with UNSCR 1373. Under this act, Jamaica has the authority to identify, freeze and seize terrorist finance related assets. Jamaica has not encountered any misuse of charitable or non-profit entities as conduits for the financing of terrorism. Jamaica has signed and ratified the UN International Convention for the Suppression of the Financing of Terrorism. Additionally, the Ministry of Foreign Affairs and Foreign Trade circulates, to all relevant agencies, the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list. To date, no accounts owned by those included on the consolidated list have been discovered in Jamaica. The Terrorism Prevention Act is not expected to become law in the near future.

Jamaica and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995. Jamaica is a party to the 1988 UN Drug Convention, the Inter-American Convention against Corruption, and the UN Convention against Transnational Organized Crime. Jamaica is also a member of the Caribbean Financial Action Task Force and the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering.

The progress the GOJ has made in fighting money laundering is tempered by stalled legislation. A more aggressive effort is necessary to bring its regime into line with international standards.

Japan

Japan is a large and important world financial center. Although the Japanese government continues to strengthen legal institutions to permit more effective enforcement of financial transaction laws, Japan still faces substantial risk of money laundering by organized crime and other domestic and international criminal elements. The principal sources of laundered funds are narcotics trafficking and financial crimes (illicit gambling, loan-sharking, extortion, abuse of legitimate corporate activities, internet fraud schemes, and all types of property-related crimes), often linked to Japan's organized criminal organizations. The National Police Agency of Japan estimates the aggregate annual income from organized criminal organizations is approximately $10 billion, $3.38 billion of which is income from the trafficking of methamphetamine.

U.S. law enforcement investigations periodically show a link between drug-related money laundering activities in the United States and bank accounts in Japan. The number of Internet-related money laundering cases is increasing. In some cases, criminal proceeds were concealed in bank accounts obtained through an Internet market. Laws enacted in 2004 now make online sales of bank accounts illegal.

The Financial Services Agency (FSA) and Ministry of Finance are working on measures, expected to be promulgated in 2006, to enable authorities to more closely monitor domestic and international money remittances. In a related move, the Cabinet office published a counterterrorist action plan on December 10, 2004 that states Japan’s intention to fully implement certain Financial Action Task Force Special Recommendations on Terrorist Financing by the end of June 2006. Specific measures will be announced this year.

On November 17, 2005, the Japanese Government’s (GOJ) headquarters for the Promotion of Measures Against Transnational Organized Crime and Other Relative Issues and the headquarters for International Terrorism agreed that relevant ministries would submit a bill to the 2007 ordinary session of the Diet to enhance compliance with the revised FATF Forty Recommendations and the FATF Nine Special Recommendations on Terrorist Financing.

Drug-related money laundering was first criminalized under The Anti-Drug Special Law that took effect in July 1992. This law also mandates the filing of suspicious transaction reports for suspected proceeds of drug offenses, and authorizes controlled drug deliveries. The legislation also creates a system to confiscate illegal profits gained through drug crimes. The seizure provisions apply to tangible and intangible assets, direct illegal profit, substitute assets, and criminally derived property that have been commingled with legitimate assets.

The narrow scope of the Anti-Drug Special Law and the burden required of law enforcement to prove a direct link between money and assets to specific drug activity limits the law’s effectiveness. As a result, Japanese police and prosecutors have undertaken few investigations and prosecutions of suspected money laundering. Many Japanese officials in the law enforcement community, including Japanese Customs, believe that Japan’s organized crime groups have been taking advantage of this limitation to launder money.

Japan expanded its money laundering law beyond narcotics trafficking to include money laundering predicates such as murder, aggravated assault, extortion, theft, fraud, and kidnapping when it passed the 1999 Anti-Organized Crime Law, which took effect in February 2000. The law also extends the confiscation laws to include the additional money laundering predicate offenses and value-based forfeitures. It also authorizes electronic surveillance of organized crime members, and enhances the suspicious transaction reporting system.

An amendment to the Anti-Organized Crime Law was submitted on February 20, 2004 to the Diet for approval, and remains under consideration. The amendment would expand the predicate offenses for money laundering from approximately 200 offenses to nearly 350 offenses, with almost all offenses punishable by imprisonment.

Japan’s Financial Services Agency (FSA) supervises public-sector financial institutions and securities transactions. The FSA classifies and analyzes information on suspicious transactions reported by financial institutions, and provides law enforcement authorities with information. Japanese banks and financial institutions are required by law to record and report the identity of customers engaged in large currency transactions. There are no secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement authorities.

To facilitate the exchange of information related to suspected money laundering activity, the FSA established the Japan Financial Intelligence Office (JAFIO) on February 1, 2000, as Japan’s financial intelligence unit. Financial institutions in Japan forward suspicious transaction reports (STRs) to JAFIO, which analyzes and disseminates STRs as appropriate. At the end of 2005, the GOJ announced plans to transfer JAFIO from the FSA to the National Police Agency, possibly in April 2007.

In 2005, JAFIO received 98,935 STRs, up slightly from the 95,315 STRs received in 2004. Of these, JAFIO disseminated 66,812 STRs to law enforcement authorities in 2005. Some 86 percent of the reports were submitted by banks, 7 percent by credit cooperatives, 4.6 percent from the country's large postal savings system, 1.2 percent from non-bank money lenders, and almost none from insurance companies.

JAFIO concluded international cooperation agreements during 2004 with Singapore's Financial Intelligence Unit (FIU) and with FinCEN, establishing cooperative frameworks for the exchange of financial intelligence related to money laundering and terrorist financing. JAFIO already had similar agreements in place with the FIUs of the United Kingdom, Belgium, and South Korea. In terms of international information exchange on money laundering, in 2004, JAFIO received 75 requests for information from foreign FIUs and provided responses to 70 of the requests.

Japanese financial institutions have cooperated with law enforcement agencies, including U.S. and other foreign government agencies investigating financial crimes related to narcotics. In 2003, the United States and Japan concluded a Mutual Legal Assistance Treaty (MLAT). Although Japan has not adopted "due diligence" or "banker negligence" laws to make individual bankers legally responsible if their institutions launder money, there are administrative guidelines that require due diligence. Japanese law protects bankers and other financial institution employees who cooperate with law enforcement entities.

In April 2002, the Diet enacted the Law on Customer Identification and Retention of Records on Transactions with Customers by Financial Institutions (a "know your customer" law). The law reinforced and codified the customer identification and record keeping procedures that banks had practiced for years. The Foreign Exchange and Foreign Trade Law was also revised so that financial institutions are required to make positive customer identification for both domestic transactions and transfers abroad in amounts of more than two million yen (approximately $19,230). Banks and financial institutions are required to maintain customer identification records for seven years.

In 2004, the FSA cited Citibank Japan's failure to properly screen clients under anti-money laundering mandates as one of a list of problems that caused the FSA to shut down Citibank Japan's private banking unit banking unit. In February 2004, the FSA disciplined Standard Chartered Bank for failing to properly check customer identities and for violating the obligation to report suspicious transactions.

The Foreign Exchange and Foreign Trade Law requires travelers entering and departing Japan to report physically transported currency and monetary instruments (including securities and gold weighing over one kilogram) exceeding one million yen (approximately $9,615), or its equivalent in foreign currency, to customs authorities. Failure to submit a report, or submitting a false or fraudulent one, can result in a fine of up to 200,000 yen (approximately $1,923) or six months' imprisonment.

In response to the events of September 11, 2001, the FSA used the anti-money laundering framework provided in the Anti-Organized Crime Law to require financial institutions to report transactions where funds appeared either to stem from criminal proceeds or to be linked to individuals and/or entities suspected to have relations with terrorist activities. The 2002 Act on Punishment of Financing of Offenses of Public Intimidation added terrorist financing to the list of predicate offenses for money laundering, and provided for the freezing of terrorism-related assets. It was enacted in July 2002. Japan signed the UN International Convention for the Suppression of the Financing of Terrorism on October 30, 2001, and became a party on June 11, 2002. After September 11, 2001, Japan has regularly searched for and designated for asset freeze any accounts that might be linked to all the suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list.

Underground banking systems operate widely in Japan, especially in immigrant communities. Such systems violate the Banking Law and the Foreign Exchange Law. The police have investigated 35 underground banking cases in which foreign groups transferred illicit proceeds to foreign countries. The aggregate value of such transfers has amounted to 420 billion yen (approximately $4 billion) since the beginning of 1992. About 120 billion yen ($1.1 billion) have been illegally transferred to China and Korea, and about 90 billion yen ($865 million) to Peru. In November 2004, the Diet approved legislation banning the sale of bank accounts, in a bid to prevent the use of purchased accounts for fraud or money laundering.

Japan has not enacted laws that allow for sharing of seized narcotics assets with other countries. However, the Japanese Government cooperates with efforts by the United States and other countries to trace and seize assets, and makes use of tips on the flow of drug-derived assets from foreign law enforcement efforts, to trace funds and seize bank accounts.

Japan is a party to the 1988 UN Drug Convention and has signed but not ratified the UN Transnational Organized Crime Convention. Japan is a member of the Financial Action Task Force. JAFIO became a member of the Egmont Group of FIUs in 2000. Japan has also taken a leadership role as a member in the Asia/Pacific Group on Money Laundering. In 2002, Japan's FSA and the U.S. Securities and Exchange Commission and Commodity Futures Trading Commission signed a nonbinding Statement of Intent (SOI) concerning cooperation and the exchange of information related to securities law violations. In January 2006 the FSA and the U.S. SEC and CFTC signed an amendment to their SOI to include financial derivatives.

The Government of Japan has many legal tools and agencies in place to successfully detect, investigate, and combat money laundering. In order to strengthen its anti-money laundering regime, Japan should stringently enforce the Anti-Organized Crime Law. Japan should also enact penalties for noncompliance with the Foreign Exchange and Foreign Trade Law, adopt measures to share seized assets with foreign governments, and enact banker "due diligence" provisions. The GOJ should also become a party to the UN Transnational Organized Crime Convention.

Jersey

The Bailiwick of Jersey (BOJ), one of the Channel Islands, is a Crown Dependency of the United Kingdom. The Islands are known as Crown Dependencies because the United Kingdom is responsible for their defense and international relations. Jersey's sophisticated array of offshore services is similar to that of international financial services centers worldwide.

In 2005, the financial services industry consists of 50 banks; 953 trust companies, 157 insurance companies (which are largely captive insurance companies); and 833 (2004 statistic) collective investment funds. Other services include investment advice, dealing, and management companies, and mutual fund companies. In addition the financial services, companies offer corporate services, such as special purpose vehicles for debt restructuring and employee share ownership schemes. For high net worth individuals, there are many wealth management services. Due to Jersey's investment services, most of the illicit money in Jersey is derived from foreign criminal activity. Domestically, local drugs trafficking and corruption of politically exposed persons (PEP) are sources of illicit proceeds found in the country. In 2004 and 2005, joint operations between Police and Customs led to the apprehension and prosecution of several local drug syndicates. Money laundering mostly occurs with Jersey's banking system, investment companies, and local Trust companies.

The International Monetary Fund (IMF) conducted an assessment of the anti-money laundering regime of Jersey in October 2003. The IMF found Jersey's Financial Services Commission (JFSC), the financial services regulator, to be in compliance with international standards, but it provided recommendations for improvement in three areas.

The Jersey Finance and Economics Committee is the government body responsible for administering the law regulating, supervising, promoting, and developing the Island's finance industry. The IMF notes that the Finance and Economics Committee's power to give direction to the JFSC could appear as a conflict of interest between the two agencies, and suggests that a separate body be established to speak for the industry's consumers. The IMF's second proposal is the establishment of rules for banks dealing with market risk, along with a code of conduct for collective investment funds. Third, the IMF recommends that a contingency plan be established for the failure of a major institution.

Jersey is currently addressing the issues and has already published the rules for collective investment funds. The JFSC intends to continue strengthening the existing regulatory powers with amendments to the Financial Services Commission Law 1998, to provide legislative support for its inspections, and the introduction of monetary fines for administrative and regulatory breaches. The amendments will also include stricter codification of industry guidelines and tighter enforcement of anti-money laundering and terrorist financing controls. The next IMF inspection is planned for 2006.

Jersey's main anti-money laundering laws are: the Drug Trafficking Offenses (Jersey) Law of 1988, which criminalizes money laundering related to narcotics trafficking, and the Proceeds of Crime (Jersey) Law, 1999, which extends the predicate offenses for money laundering to all offenses punishable by at least one year in prison. The Prevention of Terrorism (Jersey) Law 1996, which criminalizes money laundering related to terrorist activity, was replaced by the Terrorism (Jersey) Law 2002, that came into force in January 2003. The Terrorism (Jersey) Law 2002 is a response to the events of September 11, 2001, and enhances the powers of the Island authorities to investigate terrorist offenses, to cooperate with law enforcement agencies in other jurisdictions, and to seize assets. The Corruption (Jersey) Law 2005 was passed in alignment with the Council of Europe Criminal Law Convention on Corruption. The new corruption law is expected to be implemented in the spring of 2006.

The JFSC has issued anti-money laundering Guidance Notes that the courts take into account when considering whether or not an offense has been committed under the Money Laundering Order. Upon conviction of money laundering, a person could receive imprisonment of one year or more. The reporting of suspicious transactions is mandatory under the narcotics trafficking, terrorism, and anti-money laundering laws. There is no threshold for filing a suspicious transaction report, and the reporting individual is protected from criminal and civil charges by law. Banks and other financial service companies must maintain financial records of their customers for a minimum of 10 years after completion of business.

After consultation with the financial services industry, the JFSC issued a position paper (jointly issued with Guernsey and the Isle of Man) that sets out a number of proposals for further tightening the essential due diligence requirements that financial institutions should meet regarding their customers. The position paper states the JFSC's intention to insist, inter alia, on the responsibility of all financial institutions to verify the identity of their customers, regardless of the action of intermediaries. The paper also states an intention to require a progressive program to obtain verification documentation for customer relationships established before the Proceeds of Crime (Jersey) Law came into force in 1999. Each year working groups review specific portions of these principles and draft Anti-Money Laundering Guidance Notes to incorporate changes.

Approximately 30,000 Jersey companies are registered with the Registrar of Companies, who is the Director General of the JFSC. In addition to public filing requirements relating to shareholders, the JFSC requires details of the ultimate individual beneficial owner of each Jersey-registered company to be filed, in confidence, with the Commission. That information is available, under appropriate circumstances and in accordance with the law, to U.S. and other investigators.

In addition, a number of companies that are registered in other jurisdictions are administered in Jersey. Some companies, known as "exempt companies," do not have to pay Jersey income tax and are only available to nonresidents. Jersey does not provide "offshore" licenses. All regulated individuals are equally entitled to sell their services to residents and nonresidents alike. All financial businesses must have a presence in Jersey, and management must be in Jersey.

Jersey has established a Financial Intelligence Unit (FIU) known as the Joint Financial Crime Unit (JFCU). This unit is responsible for receiving, investigating, and disseminating suspicious transaction reports (STRs). The unit includes Jersey Police and Customs officers, as well as a financial crime analyst. In 2003 the JFCU received 1,272 suspicious transaction reports; 1,248 in 2004; and 1,162 in 2005. Approximately 25 percent of the STRs filed in 2004 and 2005 resulted in further police investigations. The JFCU is a member of the Egmont Group.

On July 1, 2005, the European Union Savings Tax Directive (ESD) came into force. The ESD is an agreement between the Member States of the European Union (EU) to automatically exchange information with other Member States about EU tax resident individuals who earn income in one EU Member State but reside in another. Although not part of the EU, the three UK Crown Dependencies (Jersey, Guernsey and Isle of Man) have voluntarily agreed to apply the same measures to those in the ESD and have elected to implement the withholding tax option (also known as the 'retention tax option') within the Crown Dependencies.

Under the retention tax option, each financial services provider will automatically deduct tax from interest and other savings income paid to EU resident individuals. The tax will then be submitted to local and Member States tax authorities annually. The tax authorities receive a bulk payment but do not receive personal details of individual customers. If individuals elect the exchange of information option, then no tax is deducted from their interest payments but details of the customer's identity, residence, paying agent, level and time period of savings income received by the financial services provider will be reported to local tax authorities where the account is held and then forwarded to the country where the customer resides. In 2005, the JFCU received 137 disclosures relating to individuals who had opted to select the 'retention tax option' of the ESD.

Jersey does not circulate the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, the EU designated list, or other government's designated list. However, Jersey institutions are expected to gather information of designated entities from the Internet and other public sources. Alternate remittance systems do not appear to be prevalent in Jersey.

The JFIU, in conjunction with the Attorney Generals Office, trace, seize and freeze assets. A confiscation order can be obtained if the link to a crime is proven. If the criminal has benefited from a crime, legitimate assets can be forfeited to meet a confiscation order. There is no period of time ascribed to the action of freezing until the assets are released. Frozen assets are confiscated by the Attorney Generals Office on application to the Court. Proceeds from asset seizures and forfeitures are placed in two funds. Drug trafficking proceeds go to one fund, and the proceeds of other crimes go to the second fund. The drug trafficking funds are used to support harm reduction programs, education initiatives, and to assist law enforcement in the fight against drug trafficking. Only limited civil forfeiture is allowed in relation to cash proceeds of drug trafficking located at the ports. Jersey is currently considering the introduction of civil asset forfeiture powers.

Jersey has extensive powers to cooperate with other law enforcement and regulatory agencies and regularly does so. The JFSC is also able to cooperate with regulatory authorities, for example, to ensure that financial institutions meet anti-money laundering obligations. In 2005, the JFSC and the Jersey FIU worked together in order to deny the licensing of a Trust company and close a medium size business for failure to adhere to the AML legislation and guidance issued by the regulator. The JFSC reached agreements on information exchange with securities regulators in Germany, France, and the United States. The JFSC has a memorandum of understanding for information exchange with Belgium. The 1988 Agreement Concerning the Investigation of Drug Trafficking Offenses and the

Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking, as amended in 1994, were extended to Jersey in 1996. Application of the 1988 UN Drug Convention was extended to Jersey on July 7, 1997. Jersey authorities have also put in place sanction orders freezing accounts of individuals connected with terrorist activity.

The Government of Jersey has established an anti-money laundering program that in some instances, such as the regulation of trust company businesses and the requirement for companies to file beneficial ownership with Jersey's Financial Services Commission (JFSC) go beyond what international standards require, in order to directly address Jersey's particular vulnerabilities to money laundering. Jersey should establish reporting requirements for the cross-border transportation of currency and monetary instruments. Jersey should continue to demonstrate its commitment to fighting financial crime by enhancing its anti-money laundering/counterterrorist financing regime in areas of vulnerability.

Jordan

Jordan is not a regional or offshore financial center and is not considered a major venue for international criminal activity. The banking and financial sectors, including moneychangers, are supervised by competent authorities according to international standards. The Central Bank of Jordan, which regulates foreign exchange transactions, issued anti-money laundering regulations designed to meet the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering in August 2001. Under Jordanian law, money laundering is considered an "unlawful activity" subject to criminal prosecution.

An October 8, 2001 revision to the Penal Code criminalized terrorist activities, specifically including financing of terrorist organizations. Jordan reports that it has checked for assets of the suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanctions Committee's consolidated list, although no such assets have been identified to date. In December 2004, the United States and Jordan signed an Agreement regarding Mutual Assistance between their Customs Administrations that provides for mutual assistance with respect to customs offenses and the sharing and disposition of forfeited assets.

Jordan has yet to enact a comprehensive anti-money laundering law (AML). Although Jordan's cabinet has approved the draft law, the Parliament has yet to endorse it. There is hope that Parliament will pass the law during the 2005-06 winter session. Currently, the Central Bank's suspicious transaction follow-up unit acts as a financial intelligence unit (FIU). However, the FIU's authority is only based on a regulatory (instead of legislative) foundation until an AML is passed.

Jordanian officials report that financial institutions file suspicious transactions reports and cooperate with prosecutors' requests for information related to narcotics trafficking and terrorism cases. The Central Bank of Jordan has instructed financial institutions to be particularly careful when handling foreign currency transactions, especially if the amounts involved are large or if the source of funds is in question. The Banking Law of 2000 (as amended in 2003) allows judges to waive banking secrecy provisions in any number of criminal cases, including suspected money laundering and terrorism financing.

Jordan is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Jordan has signed, but not ratified, the UN Convention against Transnational Organized Crime. Jordan is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004. The MENAFATF is a FATF-style regional body. The creation of the MENAFATF is critical for pushing the region to improve the transparency and regulatory frameworks of its financial sectors.

Jordan should enact a comprehensive anti-money laundering law. It should ratify the UN Convention against Transnational Organized Crime. Jordanian law enforcement and customs should examine forms of trade-based money laundering.

Kenya

As a regional financial and trade center for Eastern, Central, and Southern Africa, Kenya's economy has a large informal sector and a thriving network of cash-based, unrecorded transfers, primarily used by expatriates to send and receive remittances internationally. As such, Kenya is vulnerable to money laundering. Recently, Kenya has taken steps to trace millions of dollars of public funds that were laundered abroad; corruption facilitated the removal of such funds from the country.

Section 49 of the Narcotic Drugs and Psychotropic Substance Control Act of 1994 criminalizes money laundering related to narcotics trafficking. Narcotics-related money laundering is punishable by a maximum prison sentence of 14 years, though to date no clear instances of the laundering of funds from narcotics trafficking have been prosecuted. The Central Bank is the regulatory and supervisory authority for Kenya's deposit-taking institutions and has responsibility for over 51 entities. The Kenyan Parliament enacted legislation at the end of 2004 that strengthens the Central Bank's supervisory authority, but it makes no specific reference to money laundering.

In October 2000, the Central Bank issued regulations that require deposit-taking institutions to verify the identity of customers wishing to open an account or conduct a transaction. The regulations also require that these institutions report suspicious transactions. Under the regulations, banks must maintain records of large transactions and report them to the Central Bank. These regulations do not cover non-bank financial institutions such as money remitters, casinos, or investment companies, and there is no enforcement mechanism behind the regulations. Some banks do file suspicious transaction reports voluntarily, but they run the risk of civil litigation, as there are no adequate "safe harbor" provisions for reporting such transactions to the Central Bank. The trigger amount is also very high: on a daily basis, all commercial banks are required to submit reports detailing all transactions greater than $100,000. Controls on money laundering are seldom applied to financial institutions, non-bank institutions or intermediaries outside the banking sector. For example, there are casinos operating in Kenya, but they are under no obligation to file suspicious transaction reports.

Kenya has little in the way of cross-border currency controls. Kenyan regulations require that any amount of cash above $5,000 be disclosed at the point of entry or departure, but this provision is rarely enforced. Central Bank guidelines call for currency exchange firms to furnish reports on a daily basis on any single foreign exchange transaction above $10,000, and on cumulative daily foreign exchange inflows and outflows above $100,000. Under September 2002 guidelines, foreign exchange dealers are required to ensure that cross-border payments are not connected with illegal financial transactions.

The Banking Act amendment of December 2001 authorizes disclosure of financial information by the Central Bank to any monetary authority or financial regulatory authority within or outside Kenya. In 2002, the Kenya Bankers Association issued guidelines requiring banks to report suspicious transactions to the Central Bank. These guidelines do not have the force of law, and only a handful of suspicious transactions have been reported so far.

In April 2003, the Government of Kenya's (GOK) introduced the Suppression of Terrorism Bill into Parliament. The bill contains provisions that would strengthen the GOK's ability to combat terrorism. While the public does support the government's attempts to increase transparency and to combat corruption, terrorism, and money laundering, the legislation is opposed by many who fear that it could be used to commit human rights violations. A GOK official stated in October 2004 that the bill was in the process of being re-drafted. All charitable and nonprofit organizations are registered with the Government and have to submit annual reports. Noncompliance with the annual reporting requirement can lead to de-registration; however, such penalties are rarely imposed. The government did de-register some non-governmental organizations with Islamic links in 1998 in the wake of the bombing of the U.S. Embassy in Nairobi, although they were later re-registered.

At present, the government entities responsible for tracing and seizing assets include the Central Bank of Kenya Banking Fraud Investigation Unit, the Kenya Police (through the Anti-Narcotics Unit and the Anti-Terrorism Police Unit), and the Kenya Revenue Authority. The actual seizure or forfeiture of assets under current law is rare. There is currently no law authorizing the seizure of the financial assets of terrorists.

The passage of anti-money laundering legislation and the creation of a financial intelligence unit by Kenya will help to formalize its relationship with the U.S. and with other countries. In 2001, the Government of Kenya formed the Anti-Money Laundering (AML) Task Force with the mandate of drafting a comprehensive anti-money laundering law, sensitizing the public and government to money laundering issues, and addressing terrorist financing. The Task Force meets regularly to discuss AML issues.

After the inception of the task force, a bill on money laundering was drafted, and submitted to the Attorney General for final revision, but the November 21 Constitutional referendum delayed further action. In November 2005, the Attorney General had identified 21 other statutes that would need to be amended to be consistent with the AML bill. In February 2006, the World Bank, International Monetary Fund and the GOK held a workshop with stakeholders to review the draft legislation. The Task Force believes that it has clarified the issues raised by the Attorney General, and is waiting for the Attorney General to finalize the bill and send it to the Cabinet for approval and transmission to Parliament. However, uncertainties over when the President will reconvene Parliament, together with political instability generated by the eruption of multiple major corruption scandals, will likely delay further any action on the AML bill.

The key points of the legislation include tracing, seizing, and freezing suspect accounts, including those involved in the financing of terrorism; confiscation of the proceeds of crime; declaration of the source of funds; outlawing of anonymous bank accounts; and introduction of mandatory reporting of suspicious transactions above a certain amount. The proposed legislation doe not explicitly authorize the seizing of legitimate businesses used to launder money. The draft legislation provides only for criminal forfeiture.

Kenya is a party to the 1988 UN Drug Convention. In 2003, it became a party to the UN International Convention for the Suppression of the Financing of Terrorism. In 2004, it acceded to the UN Convention against Transnational Organized Crime. Kenya is an active member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. Kenya has an informal arrangement with the United States for the exchange of information regarding narcotics, terrorism financing, and other serious crime investigations. Kenya has cooperated with the United States and the United Kingdom, but lacks the institutional capacity, investigative skills, and equipment to conduct complex investigations independently.

Kenya should expedite the passage of anti-money laundering and counterterrorism legislation as first steps in building a comprehensive anti-money laundering regime. It should also establish a financial intelligence unit (FIU) to serve as a vital part of this regime. It should do a better job of enforcing the anti-money laundering laws and regulations already in force.

Korea, Democratic Peoples Republic of

For decades, citizens of the Democratic Peoples Republic of Korea (DPRK) have been apprehended trafficking in narcotics and engaged in other forms of criminal behavior, including passing counterfeit U.S. currency and trade in counterfeit products, such as cigarettes.

Substantial evidence exists that North Korean governmental entities and officials have laundered the proceeds of narcotics trafficking and have been engaged in counterfeit and other illegal activities through a network of front companies that use financial institutions in Macau for their operations. On September 20, the U.S. Department of Treasury designated Banco Delta Asia SARL in Macau as a "primary money laundering concern" under Section 311 of the USA PATRIOT Act. The Department of the Treasury noted that the bank "…has been a willing pawn for the North Korean Government to engage in corrupt financial activities through Macau." The Federal Register Notice designating the bank cited "the involvement of North Korean Government agencies and front companies in a wide variety of illegal activities, including drug trafficking and the counterfeiting of goods and currency" and noted that North Korea has been positively linked to nearly 50 drug seizures in 20 different countries since 1990, a significant number of which involved the arrest or detention of North Korean diplomats or officials.

In addition, indictments in the United States and the work of several corporate investigative teams employed by the holders of major United States and foreign cigarette and pharmaceutical trademarks have provided further compelling evidence of DPRK involvement in a wide range of criminal activities carried out in league with criminal organizations around the world, including trafficking in counterfeit branded items (cigarettes, Viagra), and high-quality counterfeit U.S. currency ("supernotes").

Korea, Republic of

South Korea is not considered an attractive location for international financial crimes or terrorist financing because of a recent legacy of foreign exchange controls. Most money laundering appears to be associated with domestic criminal activity or corruption and official bribery. Still, criminal groups based in South Korea maintain international associations with others involved in human and contraband smuggling and related organized crime. As law enforcement authorities have gained more expertise investigating money laundering and financial crimes, they have also become more cognizant of the problem.

On the whole, the South Korean Government has been a willing partner in the fight against financial crime, and has pursued international agreements toward that end. The Financial Transactions Reports Act (FTRA), passed in September 2001, requires financial institutions to report suspicious transactions to the Korea Financial Intelligence Unit (KoFIU), which operates within the Ministry of Finance and Economy. The KoFIU was officially launched in November 2001, and is composed of 60 experts from various agencies, including the Ministry of Finance and Economy, the Justice Ministry, the Financial Supervisory Commission, the Bank of Korea, the National Tax Service, the National Police Agency, and the Korea Customs Service. KoFIU analyzes suspicious transaction reports (STRs) and forwards information deemed to require further investigation to the Public Prosecutor's office, and, as of 2006, also to the Korean police.

In 2005, the government further strengthened its anti-money laundering regime by introducing mandatory currency transaction reporting (CTRs) for high-value cash transactions, on top of continued suspicious transaction reporting. Beginning in January 2006, financial institutions must report within 24 hours all cash transactions of 50 million won ($49,213) or more by individuals to KoFIU. That reporting threshold will be lowered to 30 million won ($29,528) in 2008 and to 20 million won ($19,685) in 2010. The new requirement for CTR filing will complement the existing system of suspicious transaction reporting. In January 2004 the government had already tightened its requirements for STRs by lowering the monetary threshold under which financial institutions must file STRs, to 20 million won (approximately $19,000) from the previous 50 million won. Improper disclosure of financial reports is punishable by up to five years imprisonment and a fine of up to 30 million won (about $25,000). Beginning in January 2006, financial institutions are also required to perform enhanced customer due diligence (CDD), which will strengthen previous customer identification requirements set out in the Real Name Financial Transaction and Guarantee of Secrecy Act. Under the enhanced CDD guidelines, financial institutions are required to identify and verify customer identification data such as address and telephone numbers upon account opening and when conducting transactions of 20 million won or more.

Between January 1, 2002, and August 31, 2005, KoFIU received a total of 14,665 STRs from financial institutions. The number of such cases has continued to climb noticeably each year, principally due to the lowering of the threshold for reporting suspicious transactions. For instance, in 2003, there were 1,744 STRs filed. That figure rose to 4,680 STRs in 2004, and then to 7,966 STRs in the first eight months of 2005. During this nearly four-year period, KoFIU completed analysis of 13,681 of these reports, and provided 2,090 reports to law enforcement agencies. Results were disseminated to law enforcement agencies such as the Public Prosecutor's Office (PPO), National Police Agency (NPA), National Tax Service (NTS), Korea Customs Service (KCS), and the Financial Supervisory Commission (FSC).

In December 2004, local police arrested several brokers who arranged for undocumented foreign workers to send illegal remittances abroad via the illegal underground "hawala" system. In mid-May, 2005, police arrested two Iranians on charges of arranging 60 billion won ($59 million) in illegal hawala transactions for an unknown number of their compatriots living and working in Korea. In November, 2005, ranking officers of five Mongolian banks were charged with violating bank and foreign exchange laws for running a similar illegal remittance system and for illegally operating in Korea without a banking license. The Mongolian financial firms allegedly transferred $12.1 million in funds to Mongolia from 4,200 Mongolians working in Korea. KoFIU supervises and inspects the implementation of internal reporting systems established by financial institutions. KoFIU is also charged with coordinating the efforts of other government bodies, and the Policy Coordination Committee held meetings in 2004 and 2005 to discuss policies and revisions of the FTRA. Officials charged with investigating money laundering and financial crimes are beginning to widen their scope to include crimes related to commodities trading and industrial smuggling, and continue to search for possible links of such illegal activities to international terrorist activity. On December 1, 2004, KoFIU introduced a new online electronic reporting system, through which financial institutions can report suspicious transactions more quickly.

Money laundering controls are applied to non-banking financial institutions, such as exchange houses, stock brokerages, casinos, insurance companies, merchant banks, mutual savings, finance companies, credit unions, credit cooperatives, trust companies, and securities companies. In early December, 2005, Finance Ministry officials indicated they were considering more stringent restrictions on casinos in the wake of the arrest of a Korean business executive charged with laundering 8.3 billion won ($8.17 million) to be used to bribe politicians and bureaucrats. Intermediaries such as lawyers, accountants, or broker/dealers are not covered by Korea's money laundering controls. Any traveler carrying more than $10,000 or the equivalent in other foreign currency is required to report the currency to the Korea Customs Service.

Money laundering related to narcotics trafficking has been criminalized since 1995, and financial institutions have been required to report transactions known to be connected to narcotics trafficking to the Public Prosecutor's Office since 1997. All financial transactions using anonymous, fictitious, and nominee names have been banned since the 1997 enactment of the Real Name Financial Transaction and Guarantee of Secrecy Act. The Act also requires that, apart from judicial requests for information, persons working in financial institutions are not to provide or reveal to others any information or data on the contents of financial transactions without receiving a written request or consent from the parties involved. However, secrecy laws do not apply when such information must be provided for submission to a court or as a result of a warrant issued by the judiciary.

In a move designed to broaden its anti-money laundering regime, the Republic of Korea (ROK) also criminalized the laundering of the proceeds from 38 additional offenses, including economic crimes, bribery, organized crime, and illegal capital flight, through the Proceeds of Crime Act (POCA), enacted in September 2001. The POCA provides for imprisonment and/or a fine for anyone receiving, disguising, or disposing of criminal funds. The legislation also provides for confiscation and forfeiture of illegal proceeds.

South Korea still lacks specific legislation on terrorism financing. Two versions of a new counterterrorism bill continue to languish in Korea's unicameral legislature, the National Assembly. Previous attempts to pass similar bills have not succeeded. Many politicians and nongovernmental organizations (NGOs), recalling past civil rights abuses in Korea by former administrations, oppose the passage of counterterrorism legislation because of fears about possible misuse by the National Intelligence Service. The proposed legislation is crafted to allow the Korean Government additional latitude in fighting terrorism, though general financial crimes and money laundering have already been criminalized in previously enacted laws.

The pending counterterrorism bill, if passed, would permit the government to seize legitimate businesses that support terrorist activity. Currently, under the special act against illicit drug trafficking and other related laws, legitimate businesses can be seized if they are used to launder drug money, but businesses supporting terrorist activity cannot be seized unless other crimes are committed. At this time, there are no known charitable or nonprofit entities operating in Korea that are used as conduits for the financing of terrorism.

Through KoFIU, the government circulated to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224and those listed by the European Union under relevant authorities. Korea implemented regulations on October 9, 2001, to freeze financial assets of Taliban-related authorities designated by the UN Security Council. The government then revised the regulations, agreeing to list immediately all U.S. Government-requested terrorist designations under U.S. Executive Order 13224 of December 12, 2002. No listed terrorists are known to be maintaining financial accounts in Korea at this time. Korean banks have not identified any terrorist assets. There have been no cases of terrorism financing identified since January 1, 2002.

Korean Government authorities are just beginning to assess whether the hawala system is an area of concern. Currently, gamblers who bet abroad often use alternative remittance and payment systems; however, government authorities have already criminalized those activities through the Foreign Exchange Regulation Act and other laws. Hawala-type vendors do exist in South Korea and operate primarily among the country's small population of approximately 30,000 foreigners from the Middle East and thousands more, mainly ethnic Koreans, from Mongolia, Uzbekistan, and Russia.

South Korea actively cooperates with the United States and other countries to trace and seize assets. The Anti-Public Corruption Forfeiture Act of 1994 provides for the forfeiture of the proceeds of assets derived from corruption. In November 2001, Korea established a system for identifying, tracing, freezing, seizing, and forfeiting narcotics-related and/or other assets of serious crimes. Under the system, KoFIU is responsible for analyzing and providing information on STRs that require further investigation. The Bank Account Tracing Team under the Narcotics Investigation Department of the Seoul District Prosecutor's Office (established in April 2002) is responsible for tracing and seizing drug-related assets. The Korean Government established six additional new bank account tracking teams in 2004 to serve out of the District Prosecutor's offices in the metropolitan cities of Busan, Daegu, Kwangju, Incheon, Daejon, and Ulsan, to expand its reach. Its legal framework does not allow civil forfeiture.

Korea continues to address the problem of the transportation of counterfeit international currency. The National Intelligence Service's (NIS') International Crime Center indicated that through November 2005, there were 123 reported cases of counterfeit dollars worth $269,840, compared to 141 cases of $66,525 worth in the first nine months of 2004. Bank experts confirm that the amount of forged U.S. currency is on the rise. The Korea Exchange Bank reported that the number of counterfeit $100 notes found during the first nine months of 2005—worth $190,000 total—had tripled compared to all of 2004. In April 2005, the local press reported that police arrested a Korean who had smuggled $140,000 in $100 "supernotes" from China—a record amount for South Korea.

South Korea has a number of thriving free economic zones (FEZs) that enjoy certain special privileges. However, companies operating within them are subject to the same general laws on financial transactions as companies operating elsewhere, and there is no indication these FEZs are being used in trade-based money laundering schemes or for terrorist financing. Korea mandates extensive entrance screening to determine companies' eligibility to participate in FEZ areas, and firms are subject to standard disclosure rules and criminal laws. As of December 2005, Korea had seven FEZs, as a result of the June 2004 recategorization of the three port cities of Busan, Incheon, and Kwangyang as FEZs. They were recategorized from their previous designation of "customs-free areas" in order to avoid confusion from the earlier dual system of production-focused FEZs, and logistics-oriented "customs-free zones." Incheon International Airport is slated to become the eighth FEZ.

Korea is a party to the 1988 UN Drug Convention and, in December 2000, signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. Korea is a party to the UN International Convention for Suppression of the Financing of Terrorism. The ROK also signed in December 2003, but has not ratified, the UN Convention against Corruption. Korea is an active member of the Asia/Pacific Group on Money Laundering (APG), and in 2004 hosted the APG annual meeting. Korea also became a member of the Egmont Group in 2002. An extradition treaty between the United States and the ROK entered into force in December 1999. The United States and the ROK cooperate in judicial matters under a Mutual Legal Assistance Treaty, which entered into force in 1997. In addition, the FIU continues to actively pursue information-sharing agreements with a number of countries, and had signed memoranda of understanding with 29 countries—the latest being the People's Republic of China—as of November, 2005.

The Government of the Republic of Korea should criminalize the financing and support of terrorism and should continue to move forward to adopt and implement its pending legislation. The government should extend its anti-money laundering regime to all financial intermediaries. The Republic of Korea should continue its policy of active participation in international anti-money laundering efforts, both bilaterally and in multilateral fora. Spurred by enhanced local and international concern, Korean law enforcement officials and policymakers now understand the potential negative impact of such activity on their country, and have begun to take steps to combat its growth. Their efforts will grow increasingly important due to the rapid growth and greater integration into the world economy of Korea's financial sector.

Kuwait

Kuwait, although not a major regional financial center, is experiencing unprecedented economic growth that is enhancing the country's regional financial influence. Money laundering is not believed to be a significant problem, and that which does take place is reported to be generated largely as revenues from drug and alcohol smuggling into the country and the sale of counterfeit goods.

Kuwait has nine commercial banks, including two Islamic banks, all of which provide traditional banking services comparable to Western-style commercial banks. Kuwait also has two specialized banks, the Kuwait Real Estate Bank (KREB), which is in the process of converting to an Islamic bank, and the government-owned Industrial Bank of Kuwait. Both of these banks provide medium and long-term financing. With the conversion of KREB, there will be three Islamic banks, including the Kuwait Finance House (KFH) and Bubyan Islamic Bank. As of May 31, 2004, KFH came fully under the supervision of CBK. The Bubiyan Islamic Bank was established by the Kuwaiti Investment Authority (KIA) and is in the process of being formed, after its May 2004 initial public offering. Since before the terrorist attacks of September 11, 2001, the CBK has been working on bringing Islamic financial institutions under its supervision.

The banking sector was opened to foreign competition under the 2001 Direct Foreign Investment Law, and the Central Bank of Kuwait (CBK) has already granted licenses to four foreign banks. However, while foreign banks may now operate in Kuwait, they are restricted to opening only one branch. BNP Paribas, National Bank of Abu Dhabi and HSBC are already doing business in Kuwait, while Citibank expects to begin operations in 2006.

On March 10, 2002, the Emir (Head of State) of Kuwait signed Law No. 35, which criminalizes money laundering. The law stipulates that banks and financial institutions may not keep or open any anonymous accounts or accounts in fictitious or symbolic names, and that banks must require proper identification of regular and occasional clients. The law also requires banks to keep all records of transactions and customer identification information for a minimum of five years, conduct training and establish internal control systems, and report any suspicious transactions.

Law No. 35/2002 designates the Office of Public Prosecution (OPP) as the sole authority to receive suspicious transaction reports and take appropriate action on money laundering operations. Reports of suspicious transactions are then referred from the OPP to the Central Bank of Kuwait (CBK) for analysis. The law provides for a penalty of up to seven years' imprisonment in addition to fines and asset confiscation. The penalty is doubled if an organized group commits the crime, or if the offender took advantage of his influence or his professional position. Moreover, banks and financial institutions may face a steep fine (approximately $3.3 million) if found in violation of the law. Law 35/2002 does not cite terrorist financing as a crime; however, the definition of criminal activity is broad.

The law includes articles on international cooperation, and on monitoring cash and precious metals transactions. Currency smuggling into Kuwait is also outlawed under Law No. 35/2002, although reporting requirements are not uniformly enforced at ports of entry. Provisions of Article 4 of Law No. 35/2002 state that every person shall, upon entering the country, inform the customs authorities of any national or foreign currency, gold bullion, or any other precious materials in his/her possession, valued in excess of Kuwait dinars 3,000 (approximately $10,000). However, the law does not require individuals to file customs declarations when carrying cash or precious metals out of Kuwait. The law authorizes the Minister of Finance to set forth the resolutions necessary to ensure its implementation. The Minister of Finance, as stipulated by Law No. 35/2002, can issue resolutions to enhance combating money laundering operations, without actually amending the legislation. Several cases have been opened under Law No. 35/2002, but the majority of them were closed after investigations did not disclose prosecutable offenses. Only two cases have gone to court. The cases reportedly involved money smuggling and failure to report currency transactions, and did not involve banks. Amendments to Law 35/2002 are under discussion but have yet to be finalized.

In addition to Law No. 35/2002, anti-money laundering reporting requirements and other rules are contained in the CBK's instructions No. (2/sb/92/2002), which took effect on December 1, 2002, superseding instructions No. (2/sb/50/97). The revised instructions provide for, inter alia, customer identification and the prohibition of anonymous or fictitious accounts (Articles 1-5); the requirement to keep records of all banking transactions for five years (Article 7); electronic transactions (Article 8); the requirement to investigate transactions that are unusually large or have no apparent economic or lawful purpose (Article 10); the requirement to establish internal controls and policies to combat money laundering and terrorism finance, including the establishment of internal units to oversee compliance with relevant regulations (Article 14 and 15); and, the requirement to report to the CBK all cash transactions in excess of $10,000 (Article 20). In addition, the CBK distributed detailed instructions and guidelines to help bank employees identify suspicious transactions. At the Central Bank's instructions, banks are no longer required to block assets for 48 hours on suspected accounts in an effort to avoid "tipping off" suspected accountholders. The Central Bank, upon notification from the Ministry of Foreign Affairs (MFA), issues circulars to units subject to supervision requiring them to freeze the assets of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224. Financial entities are instructed to freeze any such assets immediately and for an indefinite period of time, pending further instructions from the Central Bank, which in turn receives its designation guidance from the MFA.

In addition, CBK issued circular No. (2/sb/95/2003) in 2003, which is directed toward money changing companies (they are permitted to engage in wire transfers, selling and buying drafts and travelers' checks), and contains similar instructions with respect to combating money laundering and suspicious activities reporting guidelines. A similar order (31/2003) was issued by the Kuwait Stock Market to all companies under its jurisdiction. There are about 130 money exchange businesses (MEBs) operating in Kuwait (authorized only to exchange foreign currency), none of which are companies, and therefore, are not under the supervision of the CBK but rather under the Ministry of Commerce and Industry. The CBK has reached an agreement with the Ministry of Commerce and Industry to enforce all anti-money laundering (AML) laws and regulations in supervising such businesses. Furthermore, the Ministry will work diligently to encourage the MEBs to apply for and obtain company licenses and register with the CBK.

The Ministry of Commerce and Industry also supervises insurance agents, brokers and companies, investment companies, exchange bureaus, jewelry establishments (including gold, metal and other precious commodity traders), brokers in the Kuwait Stock Exchange, and other financial brokers. Since September 2002, these firms must abide by all regulations concerning customer identification, record keeping of all transactions for five years, establishment of internal control systems, and the reporting of suspicious transactions.

The supervision of anti-money laundering responsibilities on the part of the Ministry of Commerce and Industry is carried out by its Office of Combating Money Laundering Operations (OMLO), which was established in 2003 to improve private sector awareness and compliance with the provisions of Law No. 35/2002.The office currently has about 2,500 companies under its supervision. All new companies seeking a business license are required to receive AML awareness training from the OMLO before a license is granted. The OMLO also conducts both mandatory follow-up visits and unannounced inspections.

Businesses that are found to be in violation of provisions of Law No. 35/2002 receive an official warning from the Ministry for the first offense. The second and third violations result in closure for two weeks and one month, respectively. The fourth violation results in revocation of the license and closure of the business. Reportedly, three exchange houses were closed recently, one for operating without a license and the other two for violating instructions from the Ministry.

In April 2004, the Ministry of Finance issued Ministerial Decision No. 11 (MD No. 11/224), which transferred the chairmanship of the National Committee for Anti-Money Laundering and the Combating of the Financing of Terrorism, formerly headed by the Minister of Finance, to the Governor of the CBK. The Committee is comprised of representatives of the Ministries of Interior, Foreign Affairs, Commerce and Industry, and Finance, Labor and Social Affairs, Office of Public Prosecution, Kuwait Stock Exchange, General Customs Authority, the Union of Kuwaiti Banks, and the CBK. The National Committee is in the process of finalizing a draft legal review of Law No. 35/2002 to ensure its compliance with current international standards.

Since its inception, the National Committee has been pursuing its mandate of: drawing up the country's strategy and policy with regard to anti-money laundering and terrorist financing; drafting the necessary legislation and amendments to Law No. 35/2002, along with pertinent regulations; coordinating between the concerned ministries and agencies in matters related to combating money laundering and terrorist financing; following up on domestic, regional, and international developments and making needed recommendations in this regard; setting up appropriate channels of communication with regional and international institutions and organizations; and representing Kuwait in domestic, regional, and international meetings and conferences. In addition, the Chairman is entrusted with issuing regulations and procedures that he deems appropriate for the Committee duties and responsibilities and the organization of its activities.

In August 2002, the Kuwaiti Ministry of Social Affairs and Labor issued a ministerial decree creating the Department of Charitable Organizations. The primary responsibilities of the new department are to receive applications for registration from charitable organizations, monitor their operations, and establish a new accounting system to insure that such organizations comply with the law both at home and abroad. The Department has established guidelines for charities explaining donation collection procedures and regulating financial activities. The Department is also charged with conducting periodic inspections to insure that charities maintain administrative, accounting, and organizational standards according to Kuwaiti law. Further, the Department mandates the certification of charities' financial activities by external auditors, and limits the ability to transfer funds abroad to select charities approved by the Ministry. The Ministry also requires all fund transfers abroad to be made between authorized charity officials. Banks and money exchange businesses (MEBs) are not allowed to transfer any charitable funds outside of Kuwait without prior permission from the Ministry. In addition, any such wire transactions must be reported to the CBK, which maintains a monthly database of all transactions conducted by charities. Unauthorized public donations, including zakat (alms) collections in mosques, are also prohibited. During the 2005 Ramadan season, the Ministry introduced a new pilot program requiring charities to raise donations through the sale of government-provided coupons.

On June 23, 2003, the CBK issued Resolution No. 1/191/2003, establishing the Kuwaiti Financial Inquiries Unit (KFIU) as an independent entity within the Central Bank. The KFIU is comprised of seven part-time CBK officials and headed by the Central Bank Governor. The responsibilities of the KFIU are to receive and analyze reports of suspected money laundering from the OPP, to establish a database of suspicious transactions, to conduct anti-money laundering training, and to carry out domestic and international exchanges of information in cooperation with the OPP. Although the KFIU should act as the country's financial intelligence unit, Law No. 35/2002 did not mandate the KFIU to act as the central or sole unit for the receipt, analysis, and dissemination of suspicious transaction reports (STRs); instead, these critical functions were divided between the KFIU and OPP.

Banks in Kuwait are required to file STRs with the OPP, rather than directly with the KFIU. However, based on an MOU with the Central Bank, STRs are referred from the OPP to the KFIU for analysis. The KFIU conducts analysis and reports any findings to the OPP for the initiation of a criminal case, if necessary. The KFIU's access to information is limited, due to its inability to share information abroad without the approval of the OPP. Kuwaiti officials agree that the current limits on information sharing by the FIU are a problem that requires amending of the law, currently under revision by the National Committee.

Kuwait is a member of the Gulf Cooperation Council (GCC), which is itself a member of the Financial Action Task Force (FATF). In November 2004, Kuwait signed the memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body. Kuwait has played an active role in the MENAFATF through its participation in the drafting of regulations and guidelines pertaining to charities oversight and cash couriers. In December 2005, the CBK hosted a training seminar for those who will be conducting mutual evaluations of MENAFATF members. The Kuwait General Administration of Customs also hosted a separate conference in December 2005 on combating cash smuggling. Kuwait is a party to the 1988 UN Drug Convention. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. It has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

Kuwait is making progress in enforcing its anti-money laundering program. However, it should significantly accelerate its ongoing efforts to revise its 2002 anti-money laundering law (Law No. 35/2002), improve the sharing of financial information, strengthen the structure and responsibilities of the KFIU, secure Egmont Group membership for the KFIU, and criminalize terrorist financing. Kuwait's National Committee on Combating Money Laundering and Terrorist Financing should complete its analysis of the 2002 law and amend it to conform to current international standards. Kuwait should expand the practice of in-bound currency reporting to include all ports of entry. Kuwait should also make outbound currency and precious metals declarations mandatory. More interagency cooperation and coordination between the KFIU and other concerned parties, including Customs, could yield significant improvements in proactive investigations and international information exchange. The KFIU should be allowed to independently share financial information with its foreign counterparts, and receive, analyze, and disseminate suspicious transaction reports without obtaining prior authorization from the OPP. Kuwait should continue to enhance its charity oversight efforts, including increased coordination and diligence with third countries and organizations receiving assistance from Kuwaiti charities. Kuwait should become a party to both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism.

Laos

Laos is on the fringe of the region's banking network. Its banking sector is dominated by state-owned commercial banks in need of extensive reform. The small scale and poor financial condition of Lao banks may make them more likely to be venues for certain kinds of illicit transactions. Lao banks are not optimal for moving large amounts of money in any single transaction, due to the visibility of such movements in a small, low-tech environment. What money laundering does take place through Lao banks is likely to have been from illegal timber sales or domestic criminal activity, including drug trafficking. In a recent high-profile case involving a foreign-owned company accused of securities fraud, Lao customs authorities seized $300,000 in cash a businessman was transporting to Thailand, in contravention of Lao law. Subsequent investigation indicated that this business had transferred several million dollars from abroad through the Lao banking system in the past year, much of which was reportedly withdrawn in cash. The case revealed the weakness of the Lao banking system in monitoring suspicious transactions.

Laos has drafted a money laundering law with antiterrorism finance components, based upon a model law provided by the Asian Development Bank. The legislation was proposed during the second half of 2004 and has passed through the Ministry of Justice. It awaits prime ministerial approval and is expected to be passed by the National Assembly in April 2005, possibly with changes. The law will criminalize money laundering and terrorist financing. A Financial Intelligence Unit (FIU) will also be established, to supplant the small and informal one currently in place. Reportedly, a provision will be made for the freezing of suspect transactions and forfeiture of laundering proceeds. The Bank of Laos currently has a very small Banking Supervision Department, and it is believed the Department will be augmented and used to help implement the new legislation. Provision will be made for mutual assistance in criminal matters between Laos and other countries.

Lao law prohibits the export of the national currency, the Kip. It is likely that the currency restrictions and undeveloped banking sector encourage the use of alternative remittance systems.

The GOL is a party to the 1971 UN Convention on Psychotropic Substances and has become a party to the 1988 UN Drug Convention. The GOL participates in Association of Southeast Asian Nations (ASEAN) regional conferences on money laundering. Laos also has observer status in the Asia Pacific Anti-Money Laundering Group, and plans to join fully once its anti-money laundering law is enacted.

Laos should pass anti-money laundering and antiterrorism financing legislation. Laos should also become a party to the UN International Convention for the Suppression of Financing of Terrorism and the UN Convention against Transnational Organized Crime.

Latvia*

[*The Latvia country report was updated on March 31, 2006. See updated version.]

Latvia is a growing regional financial center that has a large number of commercial banks with a sizeable non-resident deposit base. Although these banks continue to face money laundering risks, Latvian government agencies and banks acted in 2005 to significantly strengthen the financial sector and to comply with international anti-money laundering (AML) standards. Many of the improvements addressed money laundering concerns outlined in the Notices of Proposed Rulemaking against two Latvian banks—VEF Banka and Multibanka—that was issued by the U.S. Government on April 26, 2005, under Section 311 of the USA PATRIOT Act.

Sources of laundered money in Latvia primarily involve tax evasion, but also include counterfeiting, corruption, white-collar crime, extortion, financial/banking crimes, stolen cars, contraband smuggling, and prostitution. A significant amount of the proceeds of tax evasion are believed to originate from outside of Latvia. Organized crime is thought to account for a portion of criminal proceeds that are obtained domestically.

The Government of Latvia (GOL) criminalized money laundering for all serious crimes in 1998. There are requirements for customer identification, the maintenance of records on all transactions, and the reporting of large cash transactions and suspicious transactions to the Office for the Prevention of the Laundering of Proceeds Derived from Criminal Activity (Control Service), which is Latvia's Financial Intelligence Unit (FIU).

The Law on the Prevention of Laundering of Proceeds Derived from Criminal Activity (the anti-money laundering law (AML)) requires all institutions engaging in financial transactions to report suspicious activity. On February 1, 2004, Latvia adopted amendments to the AML law that expand the scope of reporting institutions, and include auditors, lawyers, and high-value dealers, as well as credit institutions. The law lists four categories of entities obligated to report suspicious activities: participants in financial and capital markets (credit institutions, insurance companies, private pension funds, stock exchanges, brokerage companies, investment companies, credit unions, and investment consultants); organizers and holders of lotteries and gambling enterprises; companies engaged in foreign currency exchange; and individuals and companies who perform professional activities and services associated with financial transactions (money transfer services, tax consultants, auditors, auditing companies, notaries, attorneys, real estate companies, art dealers, and commodities traders). Another 2004 amendment provides for the inclusion of all offenses listed in the criminal law, including terrorism, as predicate offenses for money laundering. The amendments also provide the FIU with authority to stop transactions for up to 45 days.

In January 2005, the Council of Ministers adopted Regulation 55 that created a Council for the Prevention of Laundering of Proceeds Derived from Criminal Activity, a state-level AML body chaired by the Prime Minister. In April 2005, Latvia made it illegal for banks and individuals to ignore money laundering, and criminalized the misrepresentation of the ownership of funds. Latvia has not specifically criminalized terrorist financing. The GOL maintains that existing laws are sufficient to criminally prosecute cases of terrorist finance, although to date these laws have not been tested.

In May 2005, additional amendments to the AML and the criminal law were adopted that significantly enhanced the ability of Latvian law enforcement agencies to share information with each other and with Latvia's banking regulator, the Financial and Capital Markets Commission (FCMC). In 2005, Latvia also passed a new Criminal Procedures Code, which removed many procedural hurdles that previously made it difficult for Latvian law enforcement agencies to aggressively investigate and prosecute financial crimes. For example, prosecutors no longer need to prove "knowledge" of the criminal origin of funds before charging a person or institution with a financial crime. Reportedly, there are also plans to increase staffing levels for AML units within the Financial Police, the Economic Police, and the FIU.

In November 2005, Latvia passed legislation instituting a cross-border currency declaration requirement, which will take effect on June 30, 2006. The cash declaration law stipulates that any person crossing the Latvian border and either importing into or exporting from the customs territory of the European Union, cash (or bank notes, financial instruments, checks, bonds) equivalent to or exceeding 10,000 euros (approximately $12,300), is obligated to declare the money to a customs officer, or, where there is no customs checkpoint, to a Border Guard.

Banks are not allowed to open accounts without prior customer due diligence, and the AML law stipulates that banks must obtain client identification documents for both residents and non-residents. For legal entities, banks must collect additional information on incorporation and registration. In June 2005, sanctions against banks that violated the AML statutes were toughened to provide for fines of as much as the equivalent of $176,000.

In addition to suspicious transactions, the law also mandates institutions to report unusual transactions. Obligated entities must report single cash transactions or several related transactions, if the equivalent is 40,000 lats (approximately $70,400) or more, or if, due to indicators that suggest unusual transactions, there is cause for suspicion regarding the laundering or attempted laundering of the proceeds from crime. Financial institutions must keep transaction and identification data for at least five years after ending a business relationship with a client. If money laundering or terrorist financing is suspected, financial institutions have the ability to freeze accounts. If a financial institution finds the activity of an account questionable, it may close the account on its own initiative.

Since July 2001, the Finance and Capital Market Commission (FCMC) has served as the GOL's unified public financial services regulator, overseeing commercial banks and non-bank financial institutions, the Riga Stock Exchange, and insurance companies. The Bank of Latvia supervises the currency exchange sector. The FCMC conducts regular audits of credit institutions and will apply sanctions to companies that fail to file mandatory reports of unusual transactions. The Control Service also checks to insure that it receives matching STRs on transactions that occur between Latvian banks.

The FCMC has approved guidelines for identifying customers and unusual and suspicious transactions, as well as guidance on the internal control mechanisms that financial institutions should have in place. The FCMC has mandated that financial institutions pay closer attention to suspicious transactions, particularly those involving jurisdictions on the Financial Action Task Force's (FATF) list of Non-Cooperative Countries and Territories (NCCTs). The May 2005 amendments to the AML law gave the FCMC the ability to share information with Latvian law enforcement agencies and to receive data on potential financial crime patterns uncovered by police or prosecutorial authorities. The June 2005 amendments to the Criminal Procedures Code added a new article criminalizing the deliberate provision of false information to a credit or a financial institution about a beneficiary.

Separate from legislative and regulatory requirements, the Association of Latvian Commercial Banks (ALCB) plays an active role in setting standards on AML issues for Latvian banks. Under the leadership of the ALCB and at the urging of the FCMC, Latvian banks collectively undertook a major review of existing customer relationships in the first half of 2005, which resulted in Latvian banks closing more than 10,000 accounts connected to customers unwilling or unable to comply with enhanced due diligence requirements. In May 2004, the ALCB adopted regulations on the Prevention of Money Laundering as guidance for Latvian banks. In June 2005, the ALCB adopted a Declaration on Taking Aggressive Action against Money Laundering, which was signed by all Latvian banks. In 2005, the ACLB also adopted a voluntary measure, observed by all Latvian banks, to limit cash withdrawals from automated teller machines to 1,000 lats (approximately $1,760) per day. The ACLB guidelines are respected by member banks. In addition to acting as an industry representative to government and the regulator, the ACLB organizes regular education courses on AML/CFT issues for employees of Latvian banks.

The Control Service, Latvia's FIU, is structurally part of the Latvian Prosecutor General's Office. The Control Service has the overall responsibility to coordinate and elaborate Latvia's AML policy and assess its effectiveness. During the first 11 months of 2005, the Control Service received 24,150 reports, of which 14,436 were reports of suspicious transactions. During that same time frame, the Control Service forwarded 139 cases to law enforcement, which included information from 2,120 unusual or suspicious transactions. The Control Service received 16,128 reports in 2004, and 15,371 reports in 2003. Approximately 40 percent of the reports received in 2004 and 2005 were for suspicious transactions and 60 percent were classified as unusual transactions.

In practice, the Control Service conducts a preliminary investigation of the suspicious and unusual reports and then may pass the information on to various authorities that investigate money laundering cases. The Control Service can forward case information to: specialized Anti-Money Laundering Investigation Units of the State Police, including the Economic Police and the Office for the Combat of Organized Crime; the Financial Police (under the State Revenue Service of the Ministry of Finance); the Bureau for the Prevention and Combat of Corruption (Anti-Corruption Bureau, ACB) for crimes committed by public officials; the Security Police (for cases concerning terrorism and terrorism financing); and other law enforcement authorities.

The Prosecutor General's Office also maintains a specially-cleared staff of seven prosecutors to prosecute cases linked to money laundering. In the first 10 months of 2005, the Prosecutor General's Office referred eight criminal cases to court for criminal offenses connected to money laundering. In one court case involving seven defendants, four of them received sentences for money laundering.

The adoption of Latvia's new Criminal Procedures Code in 2005 provided additional measures for the seizure and forfeiture of assets. The law allows law enforcement authorities better identify, trace, and confiscate criminal proceeds. Investigators have the ability to initiate parallel actions for the seizure of assets recovered during criminal investigations (previously this was possible only when investigations were complete). Latvia continues to work to adapt its legislation to the Framework Decision of the Council of the European Union of July 22, 2003 (2003/577/JHA) on the Execution in the European Union of Orders for Freezing Property or Evidence. Interagency cooperation between Latvian law enforcement agencies is improving, due to new legislative amendments that allow better information sharing and increased resources to conduct investigations. Still, cooperation is best at the highest governmental levels. At the end of 2004, the Latvian Prime Minister announced plans to create a senior (ministerial) level working group on financial crime, including representatives from government ministries, law enforcement, central bank officials and the FCMC, which led to the adoption of Council of Ministers Regulation 55 that formed the Council for the Prevention of Laundering of Proceeds Derived from Criminal Activity. The Council was the driving force behind the legislative amendments passed in May 2005.

The GOL has initiated a number of measures aimed at combating the financing of terrorism. It has issued regulations to implement the sanctions imposed by UNSCR 1267 and the subsequent respective resolutions (Cabinet of Ministers' Regulation No. 437, "On the Sanction Regime of the United Nations Security Council against the Afghan Islam Emirates in the Republic of Latvia)." On October 14, 2004, Regulation No. 840 "On the Countries and International Organizations Whose Lists Include

Persons Suspected of Committing Acts of Terrorism or Complicity Therein" entered into force. The regulations require that financial institutions report to the Control Service transactions related to any suspected terrorists or terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list or on certain other terrorist lists, including those shared with Latvia by international partners. The Control Service maintains consolidated terrorist finance and watch lists and regularly sends these to financial institutions. On several occasions, Latvian financial institutions have temporarily frozen monetary funds associated with names on terrorist finance watch lists, including those issued by the U.S. Office of Foreign Assets Control (OFAC). To date, there have been no confirmed matches to names on the list. Article 17 of the AML law authorizes the Control Service to freeze the funds of persons included on one of the terrorist lists for up to six months. Any associated investigations, asset or property seizures, and forfeitures are handled in accordance with the new Criminal Procedure Code.

Only conventional money remitters (such as Western Union and Moneygram) are permitted in Latvia. The remitters work through the banks and not as separate entities. Any other type of alternative remittance service is prohibited in Latvia.

Latvia has a growing legal gambling industry. Through September 2005, the gaming industry accounted for 70,530,000 lats (approximately $124,200,000) of revenue, a 138 percent increase over the same period in 2004. In 2004, Latvia enacted a new law that restricts slot machines to defined gaming halls (places that have greater than ten gaming machines). New legislation adopted in November 2005 stipulates that no licenses can be issued for gaming businesses outside of casinos and gaming halls beginning in 2006.

The Ministry of Finance's Department of Lotteries and Gambling Supervisory Inspection regulates the gaming industry in Latvia. Casino inspectors preside over daily cash-out operations at each of the country's casinos. All casino customers must register and show proof of identification prior to entering the casino premises. Casinos and gaming halls must provide information about winnings of greater than 5,000 lats (approximately $8,800) to the Ministry of Finance and the FIU. The Ministry of Finance has statutory authority to inquire about all casino owners and officers, and it works with the FIU to review licensing applications. In the first nine months of 2005, there were 2,191 inspections, which resulted in 155 violations.

There are four special economic zones in Latvia that provide a variety of significant tax incentives for the manufacturing, outsourcing, logistics centers, and trans-shipment of goods to other free trade zones. These zones are located at the free ports of Ventspis, Riga, and Liepaja, and in the inland city of Rezekne near the Russian and Belarusian Borders. There have been instances of reported cigarette smuggling to and from warehouses in the free trade zones, as well as outside them.

Latvia participates in MONEYVAL (the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures) and underwent a second-round mutual evaluation in 2002, the results of which were discussed during the MONEYVAL committee meeting in May 2004. Latvia is currently participating in a voluntary International Monetary Fund (IMF) evaluation that will further assess the country's AML regulatory and legal framework. This assessment will also be considered as MONEYVAL's third-round evaluation of Latvia.

Latvia is a party to the UN International Convention for the Suppression of the Financing of Terrorism and eleven other multilateral counterterrorism conventions. It ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of Proceeds from Crime in 1998, and the Council of Europe Criminal Law Convention on Corruption in December 2001. A Mutual Legal Assistance Treaty (MLAT) has been in force between the United States and Latvia since 1999, and new amended extradition and MLAT agreements were signed in December 2005 (the amended agreements are awaiting ratification in Latvia). Latvia is a party to the 1988 UN Drug Convention, and it ratified the UN Convention against Transnational Organized Crime in December 2001.

The Control Service, Latvia's FIU, has been a member of the Egmont Group since 1999 and has cooperation agreements on information exchange with FIUs in Belgium, Bulgaria, Canada, the Czech Republic, Estonia, Finland, Guernsey, Italy, Lithuania, Malta, Russia, Slovenia, and Poland. In addition, Latvia has signed multilateral agreements with several EU countries to automatically exchange information between the EU financial intelligence units using FIU.NET.

The GOL made substantial improvements in its anti-money laundering and counterterrorist financing regime in 2005. It should specifically criminalize terrorist financing or ensure that existing laws allow for the efficient and effective prosecution of such activity. It should continue to implement and use the 2005 amendments to its AML law and Criminal Procedures Code to increase information sharing and cooperation between Latvian law enforcement agencies at the working level, and to strengthen its capacity and record in aggressively prosecuting and convicting those involved in financial crimes.

Lebanon

Lebanon is a financial hub for banking activities in the Middle East. It has one of the more sophisticated banking sectors in the region. The banking sector continues to record an increase in deposits. As of October 2005, there were 64 banks (54 commercial banks and ten investment banks) operating in Lebanon with total deposits of $57 billion. Four U.S. banks and bank representative offices operate in Lebanon: Citibank, American Express Bank, the Bank of New York, and JP Morgan Chase Bank.

The Central Bank (Banque du Liban) (CBL) regulates all financial institutions and money exchange houses. Banking sources emphasize that Lebanon is not a significant financial center for money laundering, but acknowledge that it does have a number of vulnerabilities. The narcotics trade is not a principal source of proceeds in money laundering. Lebanon imposes no controls on the movement of capital. It has a substantial influx of remittances from expatriate workers and family members.

Laundered criminal proceeds come primarily from domestic criminal activity. Money laundering proceeds are largely controlled by organized crime. During 2005, the banking sector has seen two cases of bank fraud consisting of embezzlement by bank employees in branch offices. There is some smuggling of cigarettes and pirated software, but this does not generate large amounts of funds that are laundered through the banking system. There is a black market for counterfeit goods and pirated software, CDs, and DVDs. Lebanese customs officials have had some recent success in combating counterfeit and pirated goods. The illicit narcotics trade is not a principal source of money laundering proceeds.

Offshore banking is not permitted in Lebanon, nor are offshore trusts or offshore insurance companies. Legislative Decree No. 46, dated June 1983, governs offshore companies. It restricts offshore companies' activity to negotiating and signing agreements concerning business carried on outside Lebanon or in the Lebanese Customs Free Zone; thus, offshore companies are barred from engaging in activities such as industry, banking, and insurance. All offshore companies must register with the Beirut Commercial Registry, and the owners of an offshore company must submit a copy of their identification. Moreover, the Registrar of the Beirut Court keeps a special register, in which all documents and information issued by the offshore company are to be retained.

There are currently two free trade zones operating in Lebanon, at the Port of Beirut and at the Port of Tripoli. The free trade zones fall under the supervision of Customs. Exporters moving goods into and out of the free zones submit a detailed manifest to Customs. If Customs suspects a transaction to be related to money laundering or terrorism finance, it reports it to Lebanon's financial intelligence unit (FIU), the Special Investigation Commission (SIC). Lebanon has no cross-border currency reporting requirements. However, since January 2003, Customs checks travelers randomly and notifies the SIC when large amounts of cash are found.

Lebanon has continued to make progress toward developing an effective money laundering and terrorism finance regime incorporating the Financial Action Task Force (FATF) Recommendations, which culminated in the FATF's removal of Lebanon from the list of Non-Cooperative Countries and Territories (NCCTs) in 2002. With Lebanon's removal from the NCCT list, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) lifted its advisory, which had instructed all U.S. financial institutions to "give enhanced scrutiny" to all transactions involving Lebanon.

In 2004, Lebanon passed a law requiring diamond traders to seek proper certification of origin for imported diamonds; the Ministry of Economy and Trade is in charge of issuing certification for re-exported diamonds. This law, designed to prevent the traffic in conflict diamonds, allowed Lebanon to join the Kimberly Process, a voluntary joint government, international diamond industry, and civil society initiative to stem the flow of rough diamonds—that are used by rebel and terrorist movements to finance their operations—through imposing extensive requirements on participants to certify the legitimate origin of rough diamonds. In August 2003, Lebanon passed a decree prohibiting imports of rough diamonds from countries that are not members of the Kimberly Process.

In 2001, Lebanon enacted Law No. 318, which created a framework for lifting bank secrecy, broadening the criminalization of money laundering beyond drugs, mandating suspicious transaction reporting, requiring financial institutions to obtain customer identification information, and facilitating access to banking information and records by judicial authorities. Under this law, money laundering is a criminal offense and punishable by imprisonment for a period of three to seven years and by a fine of no less than twenty million Lebanese pounds (approximately $13,267). The provisions of Law No. 318 expand the type of financial institutions subject to the provisions of the Banking Secrecy Law of 1956, to include institutions such as exchange offices, financial intermediation companies, leasing companies, mutual funds, insurance companies, companies promoting and selling real estate and construction, and dealers in high-value commodities. In addition, Law No. 318 requires companies engaged in transactions for high-value items (precious metals, antiquities) and real estate to report suspicious transactions.

These companies are also required to ascertain, through official documents, the identity and address of each client, and must keep photocopies of these documents as well as photocopies of the operation-related documents for a period of no less than five years. The CBL regulates private couriers who transport currency. Western Union and Money Gram are licensed by the CBL and are subject to the provisions of this law. Charitable and nonprofit organizations must be registered with the Ministry of Interior, are required to have proper corporate governance, including audited financial statements, and are subject to the same suspicious reporting requirements.

All financial institutions and money exchange houses are regulated by the CBL. Law 318 (2001) clarified the CBL's powers to: require financial institutions to identify all clients, including transient clients; maintain records of customer identification information; request information about the beneficial owners of accounts; conduct internal audits; and exercise due diligence in conducting transactions for clients.

Law No. 318 (2001) also established an FIU, called the Special Investigation Commission (SIC), which is an independent entity with judicial status that can investigate money laundering operations and monitor compliance of banks and other financial institutions with the provisions of Law No. 318. The SIC serves as the key element of Lebanon's anti-money laundering regime and has been the critical driving force behind the implementation process. The SIC is responsible for receiving and investigating reports of suspicious transactions. The SIC is the only entity with the authority to lift bank secrecy for administrative and judicial agencies, and it is the administrative body through which foreign FIU requests for assistance are processed.

Since its inception, the SIC has been active in providing support to international criminal case referrals. From January through November 2005, the SIC investigated 173 cases involving allegations of money laundering and terrorist financing activities. Out of these cases, nine were originated at U.S. Government request. Eighteen of the 173 cases were related to terrorist financing. Bank secrecy regulations were lifted in 76 instances. The SIC transmitted the 76 cases to the general state prosecutor for further investigations and to determine if these cases would be referred to the penal judge for indictment. One case relating to drug charges and involving two individuals was transmitted by the general state prosecutor to the penal judge. The general state prosecutor reported two cases to the SIC for the freezing of assets. One case involved individuals convicted of organized crime activities, and the other case involved individuals convicted of drug charges. From January to November 2005, the SIC froze the accounts of 46 individuals in eleven of the 173 cases investigated. Total dollar amounts frozen by the SIC in all these cases is about $11 million. The SIC has also worked with the UN International Independent Investigation's Commission (UNIIC) investigation into the assassination of Rafiq Hariri, helping the international inquiry lift bank secrecy laws on certain accounts and freeze the assets of suspects.

During 2003, Lebanon adopted additional measures to strengthen efforts to combat money laundering and terrorism financing, such as establishing anti-money laundering units in customs and the police. In 2003, Lebanon joined the Egmont Group of financial intelligence units. The SIC has reported increased inter-agency cooperation with other Lebanese law enforcement units, such as Customs and the police.

In order to more effectively combat money laundering and terrorist financing, Lebanon also adopted two laws important laws in 2003, Numbers 547 and 553. Law 547 expanded Article One of Law 318 (2001), criminalizing any funds resulting from the financing or contribution to the financing of terrorism or terrorist acts or organizations, based on the definition of terrorism as it appears in the Lebanese penal code (which distinguishes between "terrorism" and "resistance"). Law 547 also criminalized acts of theft or embezzlement of public or private funds, or their appropriation by fraudulent means, counterfeiting, or breach of trust, for banks and financial institutions, or falling within the scope of their activities. It also criminalized counterfeiting of money, credit cards, debit cards, and charge cards, or any official document or commercial paper, including checks. Law 553 added an article to the penal code (Article 316) on terrorist financing, which stipulates that any person who voluntarily, either directly or indirectly, finances or contributes to terrorist organizations or terrorists acts is punishable by imprisonment with hard labor for a period not less than three years and not more than seven years, as well as a fine not less than the amount contributed but not exceeding three times that amount.

In 2005, a SARC (suspicious activity report by casinos) system was put in place for the exchange of information between the SIC, customs, the internal security force (ISF) anti-money laundering and terrorist finance unit, and the general state prosecutor. The cooperation led to an increase in the number of suspicious transactions reports (STRs), and as a result, the SIC initiated several investigations in 2005.

Lebanese law allows for property forfeiture in civil as well as criminal proceedings. The Government of Lebanon (GOL) enforces existing drug-related asset seizure and forfeiture laws. Current legislation provides for the confiscation of assets the court determines to be related to or proceeding from money laundering or terrorist financing. In addition, vehicles used to transport narcotics can be seized. Legitimate businesses established from illegal proceeds after passage of Law 318 are also subject to seizure.

Lebanon was one of the founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body that promotes best practices to combat money laundering and terrorist financing in the region. It was inaugurated on November 30, 2004, in Bahrain. As it assumed its presidency for the first year, Lebanon hosted the second MENAFATF plenary in September 2005.

Lebanon has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision" and is compliant on 24 out of the 25 "Core Principles." Compliance with the pending "Core Principle" is being addressed, and a draft law providing legal protection to bank supervisors awaits the cabinet's approval. Banks are compliant with the Basel I capital accord and are preparing to comply with Basel II recommendations concerning capital adequacy.

The SIC circulates to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224 and those that European Union have designated under their relevant authorities. The SIC has signed a number of memoranda of understanding with other FIUs concerning international cooperation in anti-money laundering and combating terrorist financing. The SIC cooperates with competent U.S. authorities on exchanging records and information within the framework of Law 318.

Lebanon is a party to the 1988 UN Drug Convention, although it has expressed reservations to several sections relating to bank secrecy. It has signed and ratified the UN Convention against Transnational Organized Crime. The Government is still debating signing the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Lebanon continues to improve its efforts to develop an effective anti-money laundering and counterterrorism finance regime. The end of the Syrian military occupation in April 2005 and the gradual decline of Syrian influence over the economy (both licit and illicit), security services, and political life in Lebanon may present an opportunity for the GOL to further strengthen its efforts against money laundering, corruption and terrorist financing. The GOL should encourage more efficient cooperation between financial investigators and other concerned parties, such as police and Customs, which could yield significant improvements in initiating and conducting investigations. It should become a party to the UN International Convention for the Suppression of Terrorist Financing.

Lesotho

Lesotho is not a financial center and does not have a significant money laundering problem. There is currently no legislation criminalizing money laundering or terrorist financing. In 2003, the Government of Lesotho (GOL) drafted a "Money Laundering and Proceeds of Crime" bill. The bill was revised in 2004 and a comprehensive draft is currently under review following input by a team of advisors from the International Monetary Fund (IMF) before presentation to the Cabinet. It is hoped that the bill will be passed in 2006.

In 2005, a Pakistani businessman residing in South Africa was arrested at the airport in Lesotho for attempting to smuggle large sums of South African currency out of the country. On another occasion in 2005, a Lesotho citizen of Indian origin was also arrested at airport for carrying large sums of U.S. dollars. They were both charged with violation of the Exchange Control Regulations of the Central Bank of Lesotho.

Lesotho requires banks to know the identity of their customers and to report suspicious transactions to the Central Bank. The GOL also requires banks to report all transactions exceeding 100,000 maloti (approximately $16,000) to the Central Bank. Financial institutions are also required to maintain, for a period of ten years, all necessary records to enable them to comply with information requests from competent authorities.

The GOL created a multi-agency committee to assist in its implementation of UNSCR 1373. The Commonwealth Secretariat is assisting members of the committee to formulate national policy and draft legislation on terrorism, and intends to sponsor related training for countries of the region.

Lesotho is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Lesotho is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. However, it has not yet signed the ESAAMLG Memorandum of Understanding (MOU).

The Government of Lesotho should criminalize money laundering and terrorist financing and should develop a viable anti-money laundering regime. It should sign the MOU for ESAAMLG.

Liechtenstein

The Principality of Liechtenstein's well-developed offshore financial services sector, relatively low tax rates, liberal incorporation and corporate governance rules, and tradition of strict bank secrecy have contributed significantly to the ability of financial intermediaries in Liechtenstein to attract funds from abroad. These same factors have historically made the country attractive to money launderers. Rumors and accusations of misuse of Liechtenstein's banking system persist in spite of the progress the principality has made in its efforts against money laundering.

Liechtenstein's financial services sector includes 16 banks, three non-bank financial companies, 16 public investment companies, and a number of insurance and reinsurance companies. The three largest banks account for ninety percent of the market. Liechtenstein's 230 licensed fiduciary companies and 60 lawyers serve as nominees for or manage more than 75,000 entities (mostly corporations or trusts) available primarily to nonresidents of Liechtenstein. Approximately one third of these entities hold controlling interests in separate entities chartered outside of Liechtenstein. Laws permit corporations to issue bearer shares.

Narcotics-related money laundering has been a criminal offense in Liechtenstein since 1993, and the number of predicate offenses for money laundering has increased over time. The Government of Liechtenstein (GOL) is reviewing the Criminal Code in order to further expand the list of predicate offenses. Article 165 criminalizes laundering one's own funds and imposes penalties for money laundering. However, negligent money laundering is not addressed.

The first general anti-money laundering legislation was added to Liechtenstein's laws in 1996. Although the 1996 law applied some money laundering controls to financial institutions and intermediaries operating in Liechtenstein, the anti-money laundering regime at that time suffered from serious systemic problems and deficiencies. In response to international pressure, beginning in 2000, the GOL took legislative and administrative steps to improve its anti-money laundering regime.

Liechtenstein's primary piece of anti-money laundering legislation, the Due Diligence Act (DDA) of November 26, 2004, entered into force on February 1, 2005. The act repealed a number of prior laws, including the 1996 Due Diligence Act and its amendments. The DDA applies to banks, e-money institutions, casinos, dealers in high-value goods, and a number of other classes of entities. Along with a January 2005 ordinance (the Due Diligence Ordinance), the DDA sets out the basic requirements of the anti-money laundering regime: customer identification, suspicious transaction reporting, and record keeping. The act mandates that banks and postal institutions not engage in business relationships with shell banks nor maintain passbooks, accounts, or deposits payable to the bearer.

The GOL announced that by 2008 it would implement a new set of EU regulations requiring that money transfers above 15,000 euro ($17,678) be accompanied by information on the identity of the sender, including his or her name, address, and account number. The proposed measures will ensure that this information will be immediately available to appropriate law enforcement authorities and will assist them in detecting, investigating, and prosecuting terrorists and other criminals.

The Financial Market Authority (FMA) serves as Liechtenstein's central financial supervisory authority. Beginning operations on January 1, 2005, FMA assumed the responsibilities of several former administrative bodies, including the Financial Supervisory Authority and the Due Diligence Unit, both of which once exercised responsibility over money laundering issues. FMA reports exclusively to the Liechtenstein Parliament, making it independent from Liechtenstein's government. It oversees a large variety of financial actors, including banks, finance companies, insurance companies, currency exchange offices, and real estate brokers. FMA works closely with Liechtenstein's financial intelligence unit (FIU), the Office of the Prosecutor, and the police.

Liechtenstein's FIU, known as the Einheit fuer Finanzinformationen (EFFI), receives suspicious transaction reports (STRs) relating to money laundering and terrorist financing. The EFFI became operational in March 2001 and a member of the Egmont Group three months later. The EFFI has developed a system for STR analysis that involves internal examination, consultation with police, and a five-day period to decide whether to forward the report to prosecutors for further action. The EFFI has set up a database to analyze the STRs and has access to various governmental databases, although it cannot seek additional financial/bank information unrelated to a filed STR. The suspicious transaction reporting requirement applies to banks, insurers, financial advisers, postal services, exchange offices, attorneys, financial regulators, casinos, and other entities. The GOL has reformed its suspicious transaction reporting system to permit reporting for a much broader range of offenses than in the past and based on a suspicion rather than the previous standard of "a strong suspicion."

In 2004, the number of STRs increased by 36 percent from the previous year to 234. Of these 234 reports, the majority were submitted by banks (57 percent) and professional trustees (38 percent). As in 2003, fraud and money laundering remained the most prevalent types of offenses indicated by the entities submitting STRs to the FIU. The share of STRs involving fraud increased from 38 percent to 48 percent, while the share of STRs involving money laundering decreased from 37 percent to 20 percent.

Although the number of STRs filed by financial institutions in Liechtenstein is relatively small, they have generated several money laundering investigations. The EFFI works closely with the prosecutor's office and law enforcement authorities, as well as with a special economic and organized crime unit of the National Police known as "EWOK." When authorized to do so by a Special Investigative Judge, the police can use special investigative measures.

In 2004, the FIU forwarded 79 percent of the total number of STRs it received to prosecution authorities, up from 72 percent in 2003 and 61 percent in 2002. Three indictments have resulted from those 100 STR referrals. Most of the beneficial owners in transactions resulting in STRs were from Switzerland and Germany. With 8 percent of the total, the United States ranked third in terms of beneficial owners in STR filings. Liechtenstein itself ranked only sixth, with 4 percent of the total. The EFFI reports that about $120 million worth of suspicious money originated from the United States in 2004, compared to $260 million in 2003. The Russian Federation was the largest source of money suspected to have been criminally-generated with a total of $950 million.

In 2004, the EFFI received 119 inquiries from 16 foreign FIUs, slightly fewer than in 2003. In the same period, the EFFI submitted 134 inquiries to 14 different countries, down from 145 inquiries in 2003. The most frequent judicial cooperation requests originated from or were directed to Germany, Switzerland, and Austria.

Liechtenstein has in place legislation to seize, freeze, and share forfeited assets with cooperating countries. The Special Law on Mutual Assistance in International Criminal Matters gives priority to international agreements. Money laundering is an extraditable offense, and legal assistance is granted on the basis of dual criminality (i.e., the offense must be a criminal offense in both jurisdictions). Article 235A provides for the sharing of confiscated assets, and this has been used in practice. Liechtenstein has not adopted the EU-driven policy of reversing the burden of proof (i.e., making it necessary for the defendant to prove that he had acquired assets legally instead of the state's having to prove he had acquired them illegally).

A series of amendments to Liechtenstein law, adopted by Parliament on May 15, 2003, include a new catchall criminal offense for terrorist financing along with amendments to the Criminal Code and the Code of Criminal Procedure. Liechtenstein also has issued ordinances to implement United Nations Security Council Resolutions (UNSCRs) 1267 and 1333. Amendments to the ordinances in October and November 2001 allow the GOL to freeze the accounts of individuals and entities that were designated pursuant to these UNSCRs. The GOL updates these ordinances regularly.

On November 7, 2001, law enforcement entities in Switzerland, Liechtenstein, and Italy conducted raids and seized documents relating to Al-Taqwa and Nada Management, both of which had been designated under UNSRC 1267. Liechtenstein froze five Al-Taqwa accounts and investigated five companies. In connection with these actions, the GOL responded to a mutual legal assistance request from Switzerland and opened a domestic investigation based on money laundering and organized crime. The total value reported frozen as of December 2003 by the Liechtenstein authorities based on UNSCR 1267 is $145,300. According to the 2003 Liechtenstein report to the UN, six Taliban-related entities have been located in Liechtenstein. Their assets have been frozen and overlap with the $145,300 reported above.

The GOL has also improved its international cooperation provisions in both administrative and judicial matters. A mutual legal assistance treaty (MLAT) between Liechtenstein and the United States entered into force on August 1, 2003. The U. S. Department of Justice has acknowledged Liechtenstein's cooperation in the Al-Taqwa case and in other fraud and narcotics cases. The EFFI has in place a memorandum of understanding (MOU) with the FIUs in Belgium, Monaco, Croatia, Poland, and Georgia. Further MOUs are being prepared with Switzerland, France, Italy, San Marino, Canada, Malta, Russia, and Lithuania. Preliminary talks are being held with Germany.

Liechtenstein is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The GOL is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and the UN International Convention for the Suppression of the Financing of Terrorism. Liechtenstein has also signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Liechtenstein has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision" and has adopted the EU Convention on Combating Terrorism.

The Government of Liechtenstein has made consistent progress in addressing previously noted shortcomings in its anti-money laundering regime. It should continue to build upon the foundation of its evolving anti-money laundering and counterterrorist financing regime. Liechtenstein should accede to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Liechtenstein should require reporting of cross-border currency movements and ensure that trustees and other fiduciaries comply fully with all aspects of the new anti-money laundering legislation and attendant regulations, including the obligation to report suspicious transactions. The EFFI, the financial intelligence unit, should be given access to additional financial information. While Liechtenstein recognizes the rights of third parties and protects uninvolved parties in matters of confiscation, the government should distinguish between bona fide third parties and others.

Luxembourg

Despite its standing as the second-smallest member of the European Union (EU), Luxembourg is one of the largest financial centers in the world. Its strict bank secrecy laws allow international financial institutions to benefit from and operate a wide range of services and activities. With $1.4 trillion under management, Luxembourg is the second largest mutual fund investment center in the world, following the United States. Luxembourg is considered an offshore financial center, with foreign-owned banks accounting for a majority of the nation's total bank assets. Although there are a handful of domestic banks operating in the country, the majority of banks registered in Luxembourg are foreign subsidiaries of banks in Germany, France, and Belgium. For this reason (and also due to the proximity of these three nations to Luxembourg), a significant share of Luxembourg's suspicious transaction reports (STRs) are generated from transactions involving clients in these three countries.

As of December 2005, 154 banks, with a balance sheet total reaching 758 billion euros (approximately $893 billion), were registered in Luxembourg. In addition, as of November 2005, a total of 2,053 "undertakings for collective investment" (UCIs), or mutual fund companies, whose net assets had reached nearly 1.5 trillion euros (approximately $1.8 trillion), were operating out of Luxembourg. Luxembourg has about 15,000 holding companies, 97 insurance companies, and 260 reinsurance companies. As of September 2005, the Luxembourg Stock Exchange listed over 35,000 securities issued by nearly 4,100 entities from about 100 different countries. Legislation passed in June 2004 permits the registration of venture capital funds (société d'investissement en capital a risqué, or "SICAR"). As of December 2005, 40 SICARs had been registered.

While Luxembourg is not a major hub for illicit drug distribution, the size and sophistication of its financial center create opportunities for drug-related and other forms of money laundering and terrorist financing. According to a December 2004 International Monetary Fund (IMF) report, Luxembourg has "a solid criminal legal framework and supervisory system" to counter money laundering and terrorist financing, and is "broadly compliant with almost all of the Financial Action Task Force (FATF) Recommendations." The report also notes that Luxembourg's high level of cross-border business, obligatory banking secrecy, private banking, and "certain investment vehicles" create a challenging environment for countering money laundering and terrorist financing.

Luxembourg's financial sector laws are based to a large extent on EU directives. The Law of July 7, 1989, updated in 1998 and 2004, serves as Luxembourg's primary anti-money laundering (AML) and terrorist financing law, criminalizing the laundering of proceeds for an extensive list of predicate offenses, including narcotics trafficking. The list of predicate offenses has gradually increased over time, encompassing corruption, weapons offenses, organized crime, and fraud against the EU. Most recently, a law was passed on May 23, 2005, implementing the Council of Europe's Criminal Law Convention on Corruption, an action which made private-sector corruption a predicate offense for money laundering. Although only natural persons are currently subject to the law, a draft bill is ready for parliament's consideration in 2006 that would add legal persons to its jurisdiction.

On November 12, 2004, in an effort to bring Luxembourg into full compliance with the requirements of the EU's Council Directive 2001/97/EC on prevention of the use of the financial system for money laundering (2nd EU Money Laundering Directive), Luxembourg's parliament approved legislation updating the nation's AML laws. These legislative amendments formally transferred the requirements of Directive 2001/97/EC into domestic law. The 2004 amendments also broaden the scope of institutions subject to money laundering regulations. Under the current law, banks, pension funds, insurance brokers, UCIs, management companies, external auditors, accountants, notaries, lawyers, casinos and gaming establishments, real estate agents, tax and economic advisors, domiciliary agents, insurance providers, and dealers in high-value goods, such as jewelry and cars, are considered covered institutions. The AML law does not cover SICAR entities.

All covered entities are required to file STRs with the financial intelligence unit (FIU) and, though not legally required, are expected to send a copy of the report to their respective oversight authorities. Financial institutions are required to retain pertinent records for a minimum of five years; additional commercial rules require that certain bank records be kept for up to ten years. The AML law also contains "safe harbor" provisions that protect covered individuals and entities from legal liability when filing STRs or assisting government officials during the course of a money laundering investigation. The banking community generally cooperates with enforcement efforts to trace funds and seize or freeze bank accounts; the record of cooperation by notaries and others is still being tested, as the legislation has only been in effect for about a year.

The 2004 AML amendments contain requirements regarding financial institutions' internal AML programs. They impose stricter "know your customer" requirements, mandating their application to all new and existing customers (including beneficial owners) trading in goods worth at least 15,000 euros (approximately $17,678). If a transaction or business relationship is remotely based, the law details measures required for customer identification. Financial institutions must ensure adequate internal organization and employee training and must also cooperate with authorities, proactively monitoring their customers for potential risk. "Tipping off" is prohibited.

In late 2005, two new pieces of EU-wide legislation were issued: Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (3rd EU Money Laundering Directive) and Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the European Community. EU member states, including Luxembourg, must implement the Third Anti-Money Laundering Directive by December 15, 2007. The cash reporting regulation is directly applicable under Luxembourg's legal system and applies from June 15, 2007.

Although Luxembourg's strict bank secrecy rules may appear vulnerable to abuse by those transferring illegally obtained assets, under Luxembourg law the secrecy rules are waived in the prosecution of money laundering and other criminal cases. No court order is required to investigate otherwise secret account information in suspected money laundering cases or when a STR is filed. Financial professionals are obliged to cooperate with the public prosecutor in investigating such cases.

The Commission de Surveillance du Secteur Financier (CSSF), an independent government body under the jurisdiction of the Ministry of Finance, serves as the prudential oversight authority for banks, credit institutions, the securities market, some pension funds, and other financial sector entities covered by the country's AML and terrorist financing laws. The Luxembourg Central Bank oversees the payment and securities settlement system, and the Commissariat aux Assurances (CAA), also under the Ministry of Finance, is the regulatory authority for the insurance sector. The identities of the beneficial owners of accounts are available to all entities involved in oversight functions, including registered independent auditors, in-house bank auditors, and the CSSF. Under the direction of the Ministry of the Treasury, the CSSF has established a committee, the Comite de Pilotage Anti-Blanchiment (COPILAB), composed of supervisory and law enforcement authorities, the FIU, and financial industry representatives. The committee meets monthly to develop a common public-private approach to strengthen Luxembourg's AML regime.

No distinctions are made in Luxembourg's laws and regulations between onshore and offshore activities. Foreign institutions seeking establishment in Luxembourg must demonstrate prior establishment in a foreign country and meet stringent minimum capital requirements. Luxembourg companies must maintain a registered office in Luxembourg, and background checks are performed on all applicants. A ministerial decree published in July 2004 modified the Luxembourg Stock Exchange's internal regulations to make it easier to list offshore funds, provided the fund complies with CSSF requirements (as detailed in Circular 04/151). Also, a government registry publicly lists company directors. Although nominee (anonymous) directors are not permitted, bearer shares are permitted.

Established within Luxembourg's Ministry of Justice, the Cellule de Renseignement Financier (CRF) serves as Luxembourg's Financial Intelligence Unit (FIU), receiving and analyzing STRs while also seizing and freezing assets when necessary. While entities to which the FIU is subordinate can require it to take action against a suspect, they cannot prevent the FIU from prosecuting. Some members of the financial community continue to call for the creation of an administrative FIU body separate from the office of the public prosecutor. The CRF is responsible for providing members of the financial community with access to updated information on money laundering and terrorist financing practices. The FIU and CSSF work together in investigations involving significant money laundering cases. The CRF is among the most proactive FIUs in sharing information with colleagues from other FIUs.

In 2005, covered institutions filed a total of 831 STRs compared to a total of 943 in 2004. This figure represents a slight decrease in comparison to 2003, but considerably more than were received in 2001 and 2002. Among the 2,471 individuals involved in STRs in 2004, 383 were residents of Luxembourg, 350 of France, and 333 of Belgium. Residents of Germany, Italy, the UK, Russia, and the United States also were associated with a significant number of STRs. The majority of STRs are filed by banks.

In July 2003, Luxembourg's parliament passed a multifaceted counterterrorism financing law. The law defines terrorist acts, terrorist organizations, and terrorism financing in the Luxembourg Criminal Code. In addition, the specific crimes, as defined, will carry penalties of 15 years to life. The law also extends the definition of money laundering to incorporate certain terrorism-related crimes, and, with regard to special investigative measures, provides an exception to notification requirements in selected wiretapping cases. The November 2004 AML law amendments bring Luxembourg into compliance with the FATF's Special Recommendation IV by extending the reporting obligations of the financial sector to terrorist financing, independently from any context of money laundering. Covered institutions are required to report any transaction believed to be related to terrorist financing, regardless of the source of the funds.

The Ministry of Justice studies and reports on potential abuses of charitable and non-profit entities to protect their integrity. Justice and Home Affairs ministers from Luxembourg and other EU member states agreed in December 2005 to take into account five principles with regard to implementing FATF Special Recommendation VIII on non-profit organizations: safeguarding the integrity of the sector; dialogue with stakeholders; continuing knowledge development of the sector; transparency, accountability, and good governance; and effective, proportional oversight.

Luxembourg authorities have not found evidence of any widespread use in Luxembourg of alternative remittance systems such as hawala, black market exchanges, or trade-based money laundering. One case awaiting trial in 2005 involved a hawala transaction by a Luxembourg-based suspect using a German-based alternative remittance system. Officials comment that existing AML rules would apply to alternative remittance systems, and no separate legislative initiatives are currently being considered to formally address them. However, given recent interest by EU institutions in alternative remittance systems and wire transfers, the GOL will likely begin to implement FATF Special Recommendation VI in the first part of 2006.

Luxembourg law allows for criminal forfeitures. Funds found to be the result of money laundering can be confiscated even if they are not the proceeds of a crime. The GOL can, on a case-by-case basis, freeze and seize assets, including assets belonging to legitimate businesses used for money laundering. The government has adequate police powers and resources to trace, seize, and freeze assets without undue delay. Luxembourg cooperates with and provides assistance to foreign governments in their efforts to trace, freeze, seize and cause the forfeiture of assets. Luxembourg has a comprehensive system not only for the seizure and forfeiture of criminal assets, but also for the sharing of those assets with other governments. As of September 2005, illegal drug proceeds totaling over $22 million were frozen in Luxembourg at the request of U.S. authorities. The GOL worked with the U.S. Department of Justice throughout the year on several drug-related money laundering and asset forfeiture cases. In 2005, based on a U.S. legal assistance request, the GOL repatriated to the U.S. nearly $1,000,000 to victims of a fraud involving a former officer of Riggs Bank in Washington, D.C. Luxembourg and the United States have had a mutual legal assistance treaty (MLAT) since February 2001. In addition, in 2005 Luxembourg and the U.S. signed supplemental instruments required as part of the implementation of a U.S.-EU agreement designed to modernize extradition procedures and expand mutual legal assistance.

In an effort to identify and freeze the assets of suspected terrorists, the GOL routinely disseminates to its financial institutions the names of suspected terrorists or terrorist organizations on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O.13224. Luxembourg does not yet have domestic legal authority to designate terrorist groups. The GOL continues to work on draft legislation with regard to this issue. Authorities can and do take action against groups targeted through the EU designation process, the UN, or pursuant to bilateral requests from other countries. Under the 2004 amendments to Luxembourg's AML law, bilateral freeze requests are limited to a new maximum of three months; designations under the EU, UN, or international investigation processes continue to be subject to freezes for an indefinite time period. Upon request from the United States, Luxembourg has frozen the bank accounts of certain individuals suspected of involvement in terrorism. Luxembourg has also independently frozen several accounts, resulting in court challenges by the account holders. Since 2001, over $200 million in suspect accounts have been frozen by Luxembourg authorities pending further investigations. Most of the assets were subsequently released.

Luxembourg is a member of the FATF, and its FIU is a member of the Egmont Group. The FIU has negotiated memoranda of understanding with several countries, including Belgium, Finland, France, Andorra, Monaco, and Russia. Luxembourg is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Luxembourg has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. In 2005, Luxembourg ratified the Council of Europe's Criminal Law Convention on Corruption.

The Government of Luxembourg has enacted laws and adopted practices that help to prevent the abuse of its bank secrecy laws and has enacted a comprehensive legal and supervisory anti-money laundering and counterterrorism financing regime. Further action should be taken to address issues such as the lack of a distinct legal framework for the financial intelligence unit and the small number of money laundering investigations and prosecutions. The financial intelligence unit should work with regulatory agencies to formulate and issue substantive guidance to financial institutions on anti-money laundering trends and techniques. Luxembourg should continue to strengthen enforcement to prevent abuse of its financial sector, and should continue its active participation in international fora. Luxembourg should enact legislative amendments to address the continued use of bearer shares. It should ratify the UN Convention against Transnational Organized Crime.

Macau

Under the one country-two systems principle that underlies Macau's 1999 reversion to the People's Republic of China, Macau has substantial autonomy in all areas except defense and foreign affairs. Macau's free port, lack of foreign exchange controls, and significant gambling industry create an environment that can be exploited for money laundering purposes. In addition, Macau is a gateway to China, and can be used as a transit point to remit funds and criminal proceeds to and from China. Macau has a small economy heavily dependent on gaming, but is emerging as a financial center. Its offshore financial sector is not fully developed. Macau's international gambling industry, however, remains particularly vulnerable to money laundering.

Main money laundering methods in the financial system are wire transfers; currency exchange/cash conversion; the use of casinos to remit or launder money; and the use of nominees, trusts, family members, or third parties to transfer cash. Macau has taken several steps over the past three years to improve its institutional capacity to tackle money laundering, but still needs to pass anti-money laundering legislation and establish a financial intelligence unit (FIU). These measures will be helpful if they are passed and if the MSAR supports lead to greater enforcement of the new measures.

In 2005, the Macau Special Administrative Region Government (MSAR) submitted to the Legislative Assembly anti-money laundering legislation that would incorporate some of the aspects of the revised FATF Forty Recommendations. The legislation calls for the establishment of a financial intelligence unit (FIU); however, long-awaited details of the FIU's establishment are not included. These are expected to be finalized in implementing regulations at a later date. The 2005 money laundering bill broadened the definition of money laundering to include all serious predicate crimes that entail a maximum penalty of three years in prison, with heavier penalties for money laundering related to terrorism, illegal narcotics, and the international slave trade. The proposed legislation also allows the defendant to mitigate his criminal exposure if he "redresses" damages done to his victims prior to trial. It also mandated greater customer identification, a duty to refuse to undertake suspicious transactions, and penalties for entities failing to report suspicious transactions. However, it does not appear to criminalize "tipping off" a customer that a suspicious transaction report has been filed.

The draft legislation extended the obligation of suspicious transaction reporting to lawyers, notaries, accountants, auditors, tax consultants and offshore companies. As of December 2005, the bill was being debated in the Legislative Assembly, and the MSAR had not yet decided whether it would create a new entity as the FIU or assign new responsibilities and powers to an existing organization. In 2005, an interagency body consisting of representatives from the Monetary Authority of Macau, Macau Customs Service, Unitary Police, International Law Office, Gaming Inspection and Coordination Office, and other economic and law-enforcement agencies continued to discuss the mechanics of establishing the FIU and continued to exchange information in the FIU's absence.

In 2005, the MSAR also submitted to the Legislative Assembly a new counterterrorism bill aimed at strengthening counterterrorist financing measures. The bill, generally drafted to comply with UNSCR 1373, would make it illegal to conceal or handle finances on behalf of terrorist organizations. Individuals would be liable even if they were not members of designated terrorist organizations themselves. The legislation would also allow prosecution of persons who commit terrorist acts outside of Macau in certain cases, and would mandate stiffer penalties. However, the draft legislation does not mention how to freeze without delay terrorist assets, nor does it discuss international cooperation on terrorism financing. In January 2005, the Monetary Authority of Macau issued a circular to all banks and other authorized institutions requiring them to maintain a database of suspicious terrorists and terrorist organizations.

While Macau's proposed laws should create a more robust legal framework to combat money laundering, it will also need to enforce these laws. In an August, 2002 IMF "Assessment of the Regulation and Supervision of the Financial Sector of Macao", the IMF concluded that Macau was "materially noncompliant" with the Basel Committee's anti-money laundering principles, and recommended a number of improvements. On September 15, 2005, the U.S. Department of Treasury designated Macau-based Banco Delta Asia as a primary money-laundering concern under the USA PATRIOT Act. According to the U.S. Treasury Department, Banco Delta Asia provided financial services for more than 20 years to North Korea and has facilitated many of that regime's criminal activities, including circulating counterfeit U.S. currency.

Macau's financial system is governed by the 1993 Financial System Act and amendments, which lay out regulations to prevent use of the banking system for money laundering. It imposes requirements for the mandatory identification and registration of financial institution shareholders, customer identification, and external audits that include reviews of compliance with anti-money laundering statutes. The 1997 Law on Organized Crime criminalizes money laundering for the proceeds of all domestic and foreign criminal activities, and contains provisions for the freezing of suspect assets and instrumentalities of crime. Legal entities may be civilly liable for money laundering offenses, and their employees may be criminally liable.

The 1998 Ordinance on Money Laundering sets forth requirements for reporting suspicious transactions to the Judiciary Police and other appropriate supervisory authorities. These reporting requirements apply to all legal entities supervised by the regulatory agencies of the MSAR, including pawnbrokers, antique dealers, art dealers, jewelers, and real estate agents. In October 2002 the Judiciary Police set up the Fraud Investigation Section. One of its key functions is to receive all suspicious transaction reports (STRs) in Macau and to undertake subsequent investigations. In November 2003, the Monetary Authority of Macau issued a circular to banks, requiring that STRs be accompanied by a table specifying the transaction types and money laundering methods, in line with the collection categories identified by the Asia/Pacific Group on Money Laundering. Macau law provides for forfeiture of cash and assets that assist in or are intended for the commission of a crime. There is no significant difference between the regulation and supervision of onshore and of offshore financial activities.

The gaming sector and related tourism are critical parts of Macau's economy. Taxes from gaming comprised 75 percent of government revenue in the first ten months of 2005, while revenues from gaming increased 17 percent during the first ten months of 2005, compared with a year earlier. The MSAR ended a long-standing gaming monopoly early in 2002 when it awarded concessions to two additional operators, the U.S.-based Venetian and Wynn Corporations. The Venetian opened its first casino, the Sands, on May 18, 2004. In addition, MGM began constructing a casino in conjunction with the previous monopoly operator, Sociedade de Jogos de Macau (SJM), owned by local businessperson Stanley Ho. Wynn and MGM are scheduled to open casinos in 2006, and the Venetian will complete its flagship casino in 2007.

Under the old monopoly framework, organized crime groups were, and continue to be, associated with the gaming industry through their control of VIP gaming rooms and activities such as racketeering, loan sharking, and prostitution. The VIP rooms catered to clients seeking anonymity within Macau's gambling establishments, and were removed from official scrutiny. As a result, the gaming industry provided an avenue for the laundering of illicit funds and served as a conduit for the unmonitored transfer of funds out of China. Unlike SJM and new entrant Galaxy, the Sands does not cede control of its VIP gaming facilities to outside organizations. This approach impedes organized crime's ability to penetrate the Sands operation.

The MSAR's draft money laundering legislation includes provisions designed to prevent money laundering in the gambling industry. The legislation aims to make money laundering by casinos more difficult, improve oversight, and tighten reporting requirements. On June 7, 2004, Macau's Legislative Assembly passed legislation allowing casinos and junket operators to make loans, in chips, to customers, in an effort to prevent loan-sharking by outsiders. The law requires both casinos and junket operators to register with the government.

Terrorist financing is criminalized under the Macau criminal code (Decree Law 58/95/M of November 14, 1995, Articles 22, 26, 27, and 286). The MSAR has the authority to freeze terrorist assets, although a judicial order is required. Macau financial authorities directed the institutions they supervise to conduct searches for terrorist assets, using the list, listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. No assets were identified in 2005.

The Macau legislature passed a counterterrorism law in April 2002 that is intended to assist with Macau's compliance with UNSCR 1373. The legislation criminalizes violations of UN Security Council resolutions, including counterterrorist resolutions, and strengthens counterterrorist financing provisions. The UN International Convention for the Suppression of the Financing of Terrorism will apply to Macau when the PRC becomes a party to it.

The increased attention paid to financial crimes in Macau since the events of September 11, 2001, has led to a general increase in the number of suspicious transaction reports (STRs); however, the number of STRs remains low. Macau's Judiciary Police received 107 STRs in 2003, and 109 in 2004, and 68 in the first seven months of 2005 from individuals, banks, companies, and government agencies. Of the 109 STRs received during 2004, the Judiciary Police investigated 101 cases. From July 2004 to July 2005, the Public Prosecutors Office initiated seven money laundering legal proceedings, but the Macau Government could not provide accurate data regarding how many of these or previous cases resulted in convictions. The Judiciary Police vetted eight information requests from foreign countries during this period.

In May 2002, the Macau Monetary Authority revised its anti-money laundering regulations for banks, to bring them into greater conformity with international practices. Guidance also was issued for banks, money changers, and remittance agents, addressing record keeping and suspicious transaction reporting for cash transactions over $2,500. For such transactions, banks, insurance companies, and moneychangers must practice customer due diligence. In 2003, the Macau Monetary Authority examined all money changers and remittance companies to determine their compliance with these regulations. The Monetary Authority of Macau, in coordination with the IMF, updated its bank inspection manuals to strengthen anti-money laundering provisions. The Monetary Authority inspects banks every two years, including their adherence to anti-money laundering regulations.

The United States has no law enforcement cooperation agreements with Macau, though informal cooperation between the United States and Macau routinely takes place. The Judiciary Police have been cooperating with law enforcement authorities in other jurisdictions through the Macau branch of Interpol, to suppress cross-border money laundering. In addition to Interpol, the Fraud Investigation Section of the Judiciary Police has established direct communication and information sharing with authorities in Hong Kong and mainland China.

The Monetary Authority of Macau also cooperates internationally with other financial authorities. It has signed memoranda of understanding with the People's Bank of China, China's Central Bank, the China Insurance Regulatory Commission, the China Banking Regulatory Commission, the Hong Kong Monetary Authority, the Hong Kong Securities and Futures Commission, the Insurance Authority of Hong Kong, and Portuguese bodies including the Bank of Portugal, the Banco de Cabo Verde and the Instituto de Seguros de Portugal.

Macau participates in a number of regional and international organizations. It is a member of the Asia/Pacific Group on Money Laundering (APG), the Offshore Group of Banking Supervisors, the International Association of Insurance Supervisors, the Offshore Group of Insurance Supervisors, the Asian Association of Insurance Commissioners, the International Association of Insurance Fraud Agencies, and the South East Asia, New Zealand and Australia Forum of Banking Supervisors (SEAZA). In 2003, Macau hosted the annual meeting of the APG, which adopted the revised FATF Forty Recommendations and a strategic plan for anti-money laundering efforts in the region from 2003 to 2006. In September 2003, Macau became a party to the UN Convention against Transnational Organized Crime, as a result of China's ratification. Macau also became a party to the 1988 UN Drug Convention through China's ratification. Macau has taken a number of steps in the past three years to raise industry awareness of money laundering. During a March 2004 IMF technical assistance mission, the IMF and Monetary Authority of Macau organized a seminar for financial sector representatives on the FATF Revised Forty Recommendations. The Macau Monetary Authority trains banks on anti-money laundering measures on a regular basis.

Macau should implement and enforce existing laws and regulations, and pass and implement its pending legislation. Macau should ensure that regulations, structures, and training are put in place to prevent money laundering in the gaming industry, including implementing, as quickly as possible, the regulations it has drafted on the prevention of money laundering in casinos. The MSAR should take steps to implement the new FATF Special Recommendation Nine, adopted by the FATF in October 2004, requiring countries to implement detection and declaration systems for cross-border bulk currency movement. Macau should increase public awareness of the money laundering problem, improve interagency coordination, and boost cooperation between the MSAR and the private sector in combating money laundering. The Government of Macau should ensure that it expeditiously establishes a financial intelligence unit meeting Egmont standards for information sharing. It should expedite the drafting and issuing of implementing regulations to its anti-money laundering/counterterrorist financing laws, once enacted. The Government of Macau also should be more proactive in finding and freezing accounts related to money laundering of illegal proceeds such as from weapons proliferators and counterfeiters.

Malawi

Malawi is not a regional financial center. The Reserve Bank of Malawi (RBM), Malawi’s Central Bank, supervises the country’s six commercial banks. Some money laundering is tied to smuggling and converting remittance savings systems abroad. Under Malawi’s existing exchange control regime, foreign exchange remittances not backed by a “genuine” or official transaction are illegal; traders, therefore, use underground methods in their efforts to remit savings abroad

Financial institutions are required to record and report the identity of customers making large transactions, and banks must maintain those records for seven years. Banks are allowed, but not required, to submit suspicious transaction reports to the RBM. The RBM inspects banks’ records every quarter and has access to those records on an “as needed” basis for specific investigations.

Malawi’s current laws do not specifically criminalize money laundering, but can be used to prosecute money laundering cases. The Government of Malawi (GOM) drafted a “Money Laundering and Proceeds of Serious Crime” bill, which was first considered in Parliament’s Commerce and Industry Committee in 2003. The committee requested revisions in the proposed legislation before it is considered in the full Parliament. The draft law would criminalize money laundering related to all serious crimes. The draft law would also establish a legal framework for identifying, freezing, and seizing assets related to money laundering. The bill stipulates that the seized assets become the property of the GOM and should be used in the fight against money laundering. Reportedly, there has been no further action by the Parliament regarding the draft legislation.

While the GOM has not specifically criminalized terrorist financing, the RBM has the legal authority to identify and freeze assets suspected of involvement in terrorist financing. The RBM has circulated to the financial community the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee’s consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. The RBM continues to monitor the financial system for money laundering activity.

Malawi has signed the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) Memorandum of Understanding. Malawi is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime.

The Government of Malawi should enact comprehensive anti-money laundering legislation and counterterrorist finance legislation in order to develop viable regimes to thwart both money laundering and terrorist financing regimes as it has agreed to do as a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG). Malawi should become a party to the UN Convention against Transnational Organized Crime.